



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.151

(10/2003)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS

Public data networks – Maintenance

**Frame Relay operations and maintenance –
Principles and functions**

ITU-T Recommendation X.151

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.151

Frame Relay operations and maintenance: Principles and functions

Summary

This Recommendation defines the basic Frame Relay Operations and Maintenance Principles and Functions. The quality of Frame Relay services can be tested, measured and diagnosed using OAM frames. FR OAM frames can be used to measure the primary performance parameters of frame relay networks. OAM frames provide the ability to do in-service monitoring on both SVC and PVC connections.

This Recommendation includes a network reference model, an overview of the OAM frame structure, and OAM measurement procedures. The contents of this Recommendation are based on the reference model, the OAM protocol formats, the OAM procedures and descriptions of message flows as defined in FRF.19 – Frame Relay Operations, Administration, and Maintenance Implementation Agreement. Additionally procedures for measurement of frame delay jitter, frame loss ratio and use of loopback for fault detection are defined.

Source

ITU-T Recommendation X.151 was approved by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure on 29 October 2003.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2004

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
4 Abbreviations.....	2
5 Conventions	3
6 Reference model	3
7 OAM protocol formats	6
7.1 Encapsulation formats	6
7.2 OAM message format.....	8
7.3 OAM information fields	11
8 OAM procedures	19
8.1 Message encoding/decoding rules.....	19
8.2 General message processing.....	20
8.3 Hello message processing (device discovery).....	22
8.4 Service level verification message processing	24
8.5 Non-latching loopback message processing.....	30
8.6 Latching loopback message processing.....	31
8.7 Diagnostic indication message processing	32
8.8 Network applications of loopback.....	32
Appendix I – General receive procedures.....	34
Appendix II – Message flows	35
II.1 Discovery.....	35
II.2 FTD measurement	36
II.3 FDR/DDR measurement	37
II.4 Non-latching loopback	39
II.5 Latching loopback	40
Appendix III – Example of delivery ratio calculation	41
III.1 Ingress processing	42
III.2 Egress processing	42

ITU-T Recommendation X.151

Frame Relay operations and maintenance: Principles and functions

1 Scope

This Recommendation specifies OAM frame formats and procedures for measuring the performance of frame relay networks. OAM provides a means to test, diagnose and measure the quality of frame relay services. The protocol and procedures may be used by public frame relay networks and by service providers and/or end-users. The procedures are applicable to PVCs, as well as to the data transfer phase of SVCs.

The following clauses of this Recommendation are based on the text of FRF.19:

- Clause 6. A reference model for different networks and domains over which FR OAM measurements can be made.
- Clause 7. OAM protocol formats – Detailed structure (message formats) of FR OAM frames.
- Clause 8. OAM procedures – use of FR OAM frames to measure the primary performance parameters of frame relay services.

Appendices I, II and III – Informative text describing general receive procedures, message flows and delivery ratio calculation to aid interpretation and interoperability.

The following clauses of this Recommendation are additional to the text of FRF.19:

- Clause 8.4.3.6: Procedures for the estimation of frame delay jitter.
- Clause 8.4.4.5: Frame loss ratio calculation.
- Clause 8.8: Network applications of loopback.

NOTE – Interoperability with ATM OAM as defined by ITU-T Rec. I.610 and other OAM protocols is beyond the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.
- ITU-T Recommendation I.370 (1991), *Congestion management for the ISDN frame relaying bearer service*.
- ITU-T Recommendation I.555 (1997), *Frame Relaying Bearer Service interworking*.
- ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.
- ITU-T Recommendation X.36 (2003), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for public data networks providing frame relay data transmission service by dedicated circuit*.

- ITU-T Recommendation X.76 (2003), *Network-to-network interface between public data networks providing PVC and/or SVC frame relay data transmission service.*
- ITU-T Recommendation X.121 (2000), *International numbering plan for public data networks.*
- ITU-T Recommendation X.144 (2003), *User information transfer performance parameters for public frame relay data networks.*
- ITU-T Recommendation X.145 (2003), *Connection establishment and disengagement performance parameters for public Frame Relay data networks providing SVC services.*
- ITU-T Recommendation X.146 (2000), *Performance objectives and quality of service classes applicable to frame relay.*
- ITU-T Recommendation X.147 (2003), *Frame Relay network availability.*
- ITU-T Recommendation X.148 (2003), *Procedures for the measurement of the performance of public data networks providing the international frame relay service.*
- Frame Relay Forum Implementation Agreement 19, FRF.19 (2001), *Frame relay operations, administration, and maintenance implementation agreement.*

3 Definitions

The following terms, when used in this Recommendation, are used as defined in ITU-T Recs X.144, X.145, X.146, X.147 and X.148.

- Frame Transfer Delay
- Frame Delivery Ratio
- Data Delivery Ratio
- Frames_offered
- Frames_received
- Data_offered
- Data_received
- Availability

4 Abbreviations

This Recommendation uses the following abbreviations:

AESA	ATM End System Address
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification
CIR	Committed Information Rate
DCE	Data Circuit-terminating Equipment
DDR	Data Delivery Ratio
DE	Discard Eligibility
DLCI	Data Link Connection Identifier
DTE	Data Terminal Equipment
FDR	Frame Delivery Ratio
FECN	Forward Explicit Congestion Notification

FR	Frame Relay
FROMP	Frame Relay OAM Maintenance Point
FTD	Frame Transfer Delay
IA	Implementation Agreement
IEEE	Institute of Electrical and Electronics Engineers
IF	Information Field
IPv4	Internet Protocol Version 4
ITU	International Telecommunication Union
MTU	Maximum Transmission Unit
NLPID	Network Layer Protocol Identification
NNI	Network-to-Network Interface
OAM	Operations, Administration and Maintenance
OUI	Organizationally Unique Identifier
PHY	Physical Interface
PVC	Permanent Virtual Circuit
SLA	Service Level Agreement
SVC	Switched Virtual Circuit
UNI	User-to-Network Interface
VC	Virtual Circuit

5 Conventions

For the purposes of ensuring interoperability of OAM systems, the following terms, when used in this Recommendation and highlighted in **bold**, are used as defined in this clause:

Must, Shall, or Mandatory – the item is an absolute requirement of this Recommendation.

Should – the item is highly desirable.

May or Optional – the item is not compulsory, and may be followed or ignored according to the needs of the Recommendation.

Not Applicable – the item is outside the scope of this Recommendation.

NOTE – The abbreviation OAM is used throughout this Recommendation and has the same meaning as the abbreviation OA&M which is used throughout FRF.19.

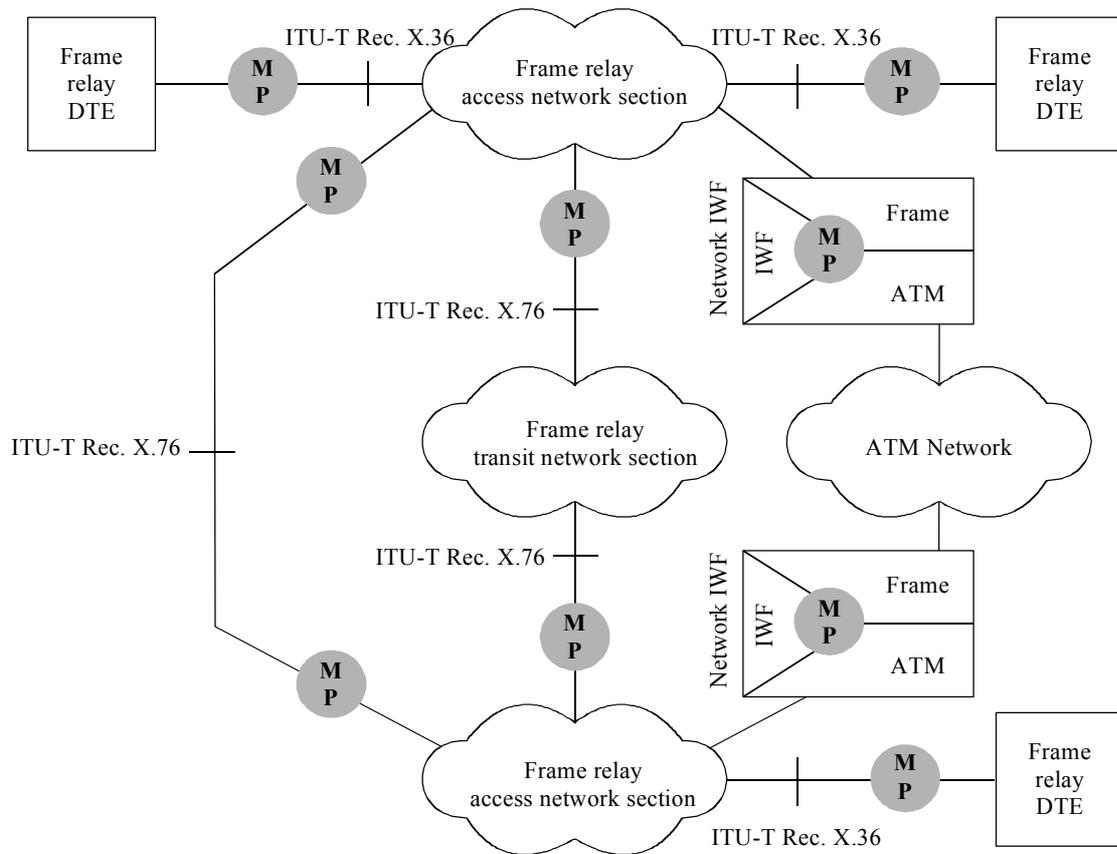
6 Reference model

Figures 1 and 2 define generic network reference models illustrating typical locations of FR OAM Maintenance Points (FROMPs). The four types of administrative domains used for FR OAM operations are also defined.

Figure 1 illustrates a reference frame relay network that is interworking with an ATM network. A number of example monitoring points are indicated. In this reference network, the following examples of circuit connections are shown:

- A VC that spans a single FR access network section.
- A VC that spans two FR access network sections connected by an NNI.

- A VC that spans two FR access network sections connected by a FR transit network.
- A VC that spans two FR access network sections connected by an ATM transit network section using network interworking.



X.151_F1

M P Example monitor point for optional frame relay OAM maintenance device (FROMP)

NOTE – Monitoring points may be external probes or embedded in DTE or DCE equipment.

Figure 1/X.151 – Network reference model

Figure 2 shows the location of OAM Maintenance Points (FROMPs) for monitoring performance across various segments of a frame relay virtual connection.

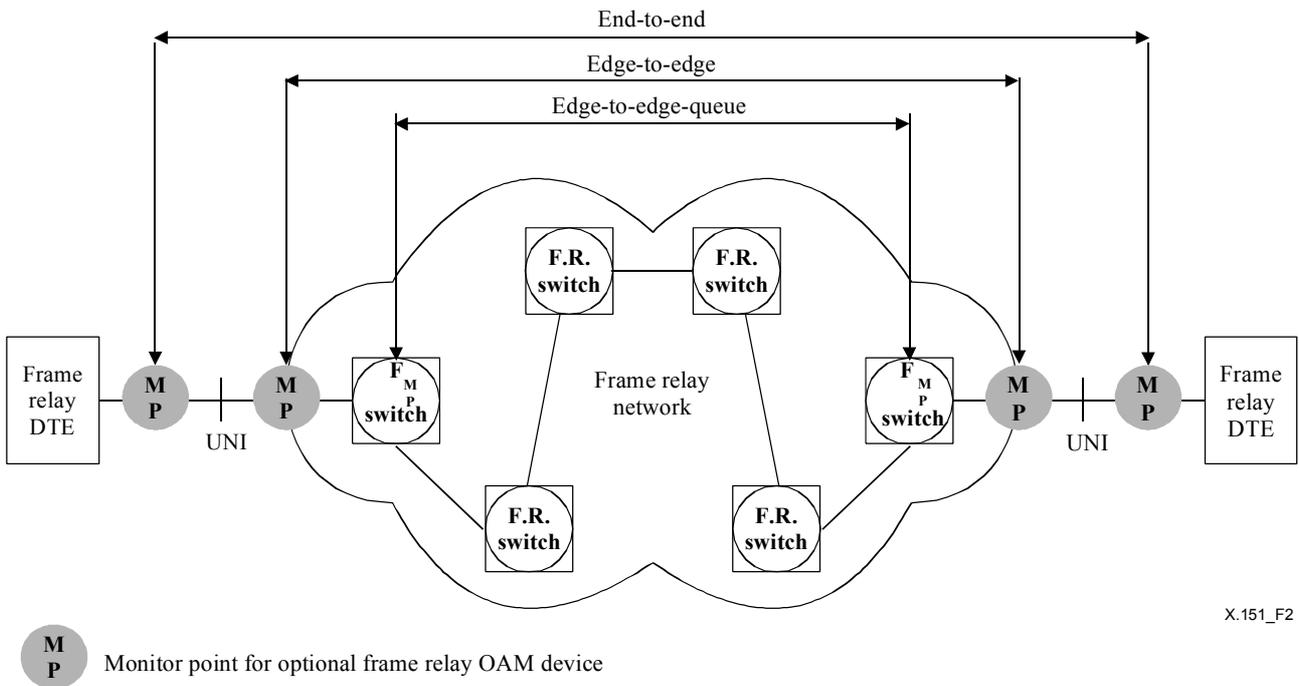


Figure 2/X.151 – Location of OAM Maintenance Points (FROMPs) for monitoring performance

A VC may consist of several sections and components administered by multiple organizations. The portions of a VC that are administered by the same organization(s) create an administrative domain. Figure 3 presents the administrative domain reference model.

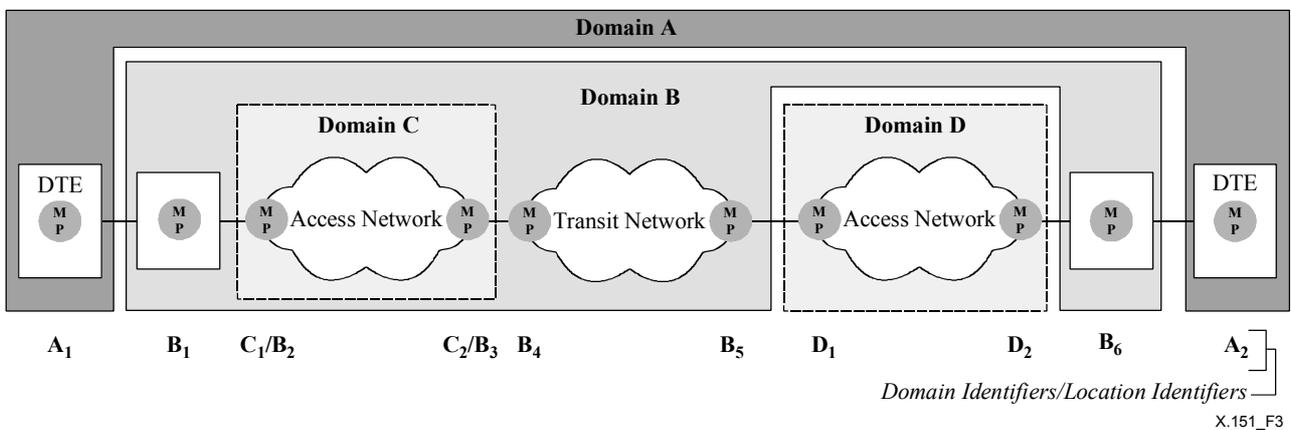


Figure 3/X.151 – Administrative domain reference model

Four different and overlapping types of administrative domains are illustrated in this model. An administrative domain may consist of any arbitrary collection of locations on the virtual circuit.

Domain A – Set of interfaces and devices administered by the end-user (locations A₁ and A₂).

Domain B – Set of interfaces and devices administered by a global service provider working with local partners in each region (locations B₁, B₂, B₃, B₄, B₅ and B₆).

Domain C – Set of interfaces and devices administered by a local partner of the global service provider (locations C_1 and C_2). A network partner has granted the global service provider permission to interrogate OAM devices operated by the local partner. This permission is reflected in multiple domain memberships (C_1/B_2 and C_2/B_3).

Domain D – Set of interfaces and devices controlled by a local partner of the global service provider (locations D_1 and D_2). The partner has refused to grant the global service provider permission to interrogate OAM devices operated by the local partner.

Administrative domains provide well-defined zones for OAM messaging. At the outermost points of an administrative domain on a given VC (see Figure 3 points B_1 and B_6 for Domain B), an administrative boundary exists to delineate the domain. All OAM messages include a domain identification, which is used to identify the intended administrative domain.

A FROMP at a domain boundary of a VC's administrative domain prevents messages intended for the domain from being forwarded beyond the domain boundary. As an example, location D_2 does not send an OAM message with a domain identification for Domain D towards B_6 .

Further, these boundary devices detect and discard counterfeit messages originating outside the administrative domain. Thus, if a rogue application at location B_5 creates a message claiming to have domain identification D and sends the message to D_1 , D_1 will discard the message to prevent an illegal OAM request from entering the domain.

Messages for other domains **must** be passed through the domain boundary in either direction without interpretation or discard. As an example, location A_1 transmits a message towards location A_2 . Location B_1 , a boundary device for Domain B, checks the administrative domain identification and verifies that the message does not claim to originate from within Domain B. The message is then forwarded onward to locations C_1 and D_1 where the same boundary checks are made. The message is then forwarded onward to location A_2 , the target of the message.

Messages received from within a domain are trusted. As an example, location B_1 in Domain B trusts messages from direction C_1 with the domain identification for Domain B because they share a common administrative domain.

The Administration/organization that controls the insertion of OAM frames in a FR management domain must ensure that those frames are extracted before they leave the span of control of that Administration/organization with the exception of those management domains that have been extended by bilateral agreements.

7 OAM protocol formats

Frame relay OAM messages are carried in standard frame relay frames. Two encapsulation formats for the data portion of these frame relay frames are defined to allow for interoperability with other traffic. The messages consist of a header portion, and one or more information fields.

The remainder of this clause describes the format of frame relay OAM protocol messages, and consists of three portions:

- An encapsulation format (see 7.1);
- An OAM message (see 7.2) containing one or more;
- OAM Information Fields (see 7.3).

NOTE – See 8.1 for rules on encoding and decoding these formats. Figures throughout this Recommendation illustrate 2-octet DLCI encoding. Both 2- and 4-octet addresses are supported in all cases.

7.1 Encapsulation formats

The frame relay OAM protocol supports two encapsulation formats. These formats allow for implementation in a variety of network elements and for compatibility with U-plane traffic formats.

Implementations **must** support the multiprotocol encapsulation format to be compliant with this Recommendation. Implementations **may** optionally support the non-UI encapsulations.

7.1.1 Multiprotocol encapsulation

The multiprotocol encapsulation format is compatible with frame relay equipment and applications. The format uses a NLPID (0xB2) to distinguish OAM traffic from U-plane traffic conforming to ITU-T Rec. X.36. Figure 4 depicts the multiprotocol encapsulation format when an X.36 2-octet header is used.

Bits								Octet
8	7	6	5	4	3	2	1	
DLCI (msb)						C/R	EA	1
x	x	x	x	x	x	0	0	
DLCI (lsb)				FECN	BECN	DE	EA	2
x	x	x	x	x	x	x	1	
Control								3 (Note)
0	0	0	0	0	0	1	1	
NLPID								4
1	0	1	1	0	0	1	0	
FR_OAM Message								5

NOTE – Control is at octet 5 when 4-octet addressing of X.36 is used.

Figure 4/X.151 – Multiprotocol encapsulation format

7.1.2 Non-UI encapsulation

The non-UI encapsulation format is designed for use with frame relay traffic that is not distinguishable from the OAM multiprotocol encapsulation format. The prime example of this is clause 5/I.555 (X.25 encapsulated) traffic. Figure 5 depicts the non-UI encapsulation format when an X.36 2-octet header is used.

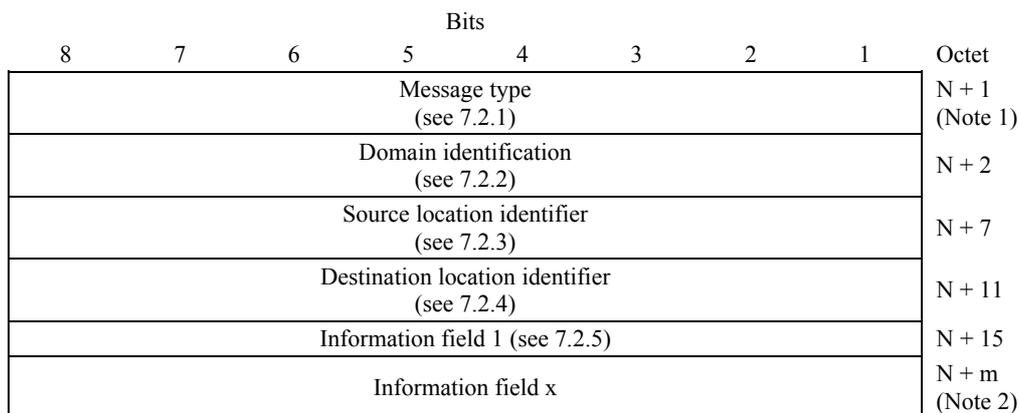
Bits								Octet
8	7	6	5	4	3	2	1	
DLCI (msb)						C/R	EA	1
x	x	x	x	x	x	0	0	
DLCI (lsb)				FECN	BECN	DE	EA	2
x	x	x	x	x	x	x	1	
Control								3 (Note)
0	0	0	0	0	0	1	0	
NLPID								4
1	0	1	1	0	0	1	0	
FR_OAM Message								5

NOTE – Control is at octet 5 when 4-octet addressing of X.36 is used.

Figure 5/X.151 – Non-UI encapsulation format

7.2 OAM message format

Figure 6 depicts the format of OAM messages.



NOTE 1 – Offset N is 4, 6, or 10, depending upon encapsulation and address size used.

NOTE 2 – Information fields are populated as needed.

Figure 6/X.151 – OAM message format

7.2.1 Message type field

The purpose of the message type field is to identify the message being sent. Values for this field are shown in Table 1.

Table 1/X.151 – OAM message type values

Message type value	Usage
0x1	Hello (see 8.3 for usage)
0x2	Service verification (see 8.4 for usage)
0x3	Non-latching loopback (see 8.5)
0x4	Latching loopback (see 8.6)
0x5	Diagnostic indication (see 8.7)

7.2.2 Domain identification

The purpose of the domain identification field is to uniquely identify the Administrative Domain to which this message belongs. This field consists of two parts, a 1-octet descriptor for the type of plan, shown in Table 2 below, followed by a 4-octet domain identifier.

Table 2/X.151 – Domain identification plan

Domain identification plan value	Usage
0x00	Reserved for future use
0x01	User defined identifier
0x02	OUI identifier
0x03	IPv4 network identifier
0x31	X.121 identifier
0x33	E.164 identifier
0xFF	Private domain identifier
NOTE 1 – User defined identifiers are for use by end-user administered equipment. NOTE 2 – OUI, IPv4, X.121 and E.164 identifiers are for use by service providers. NOTE 3 – Private domain identifiers are for use via multilateral agreement.	

The domain identification field (the combined values of the type of plan and domain identifier) **must** be unique for each administration along the path of a VC.

The format of the 4-octet domain identifier is dependent upon the value of the domain identification plan.

7.2.2.1 Domain identifier format for "User Defined" plan

The "User Defined" plan is intended for use by customer administered equipment. When the domain identification plan indicates usage of the user defined identifier, the format of the remaining 4 octets is not subject to standardization. A value of zero **may** be used as the default value to indicate the last OAM capable device on the VC.

7.2.2.2 Domain identifier format for "OUI" plan

The "OUI" plan is one of several plans intended for use by service providers. When the domain identification plan indicates usage of the OUI identifier, the format of the remaining 4 octets is created by using a zero byte followed by a 3-octet OUI. OUI identifiers are assigned and administered by the IEEE.

7.2.2.3 Domain identifier for "IPv4 Network" plan

The "IPv4" plan is also intended for use by service providers. When the domain identification plan indicates usage of the IPv4 identifier, the format of the remaining 4 octets is the network portion of a public IPv4 address block owned by the service provider. Public IPv4 addresses are administered by the IETF.

7.2.2.4 Domain identifier format for "X.121" plan

The "X.121" plan is also intended for use by service providers. When the domain identification plan indicates usage of the X.121 identifier, the value of the remaining 4 octets are created as follows:

- Take X.121 DNIC, as defined in ITU-T Rec. X.121;
- Pad on the left with zeros, as necessary, to 8 octets;
- BCD encode the result into 4 octets.

7.2.2.5 Domain identifier format for "E.164" plan

The "E.164" plan is also intended for use by service providers. When the domain identification plan indicates usage of the E.164 identifier, the value of the remaining 4 octets are created as follows:

- Take E.164 network identification field of the transit network ID, as defined in ITU-T Rec. X.76;
- Pad on the left with zeros, if necessary, to 8 octets;
- BCD encode the result into 4 octets.

7.2.2.6 Domain identifier format for "Private" plan

When the domain identification plan indicates usage of the private domain identifier, the format of the remaining 4 octets is not subject to standardization.

7.2.3 Source location identifier field

The purpose of the source location identifier field is to uniquely identify the source of an OAM message with the indicated administrative domain.

The values used in the source location identifier field **must** be unique for each administration along the path of a VC. The value of all ones is reserved and **may not** be used as a source location identifier.

The format of this 4-octet field is not subject to standardization.

7.2.4 Destination location identifier field

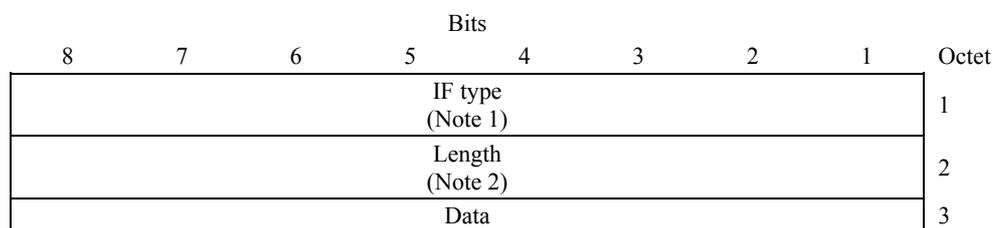
The purpose of the destination location identifier field is to uniquely identify the destination of an OAM message with the indicated administrative domain, or to indicate a broadcast destination.

The values used in the destination location identifier field **must** be unique for each administration along the path of a VC. The value of all ones is used to indicate the global (all destinations) broadcast for the identified administration.

The format of this 4-octet field is not subject to standardization.

7.2.5 OAM information field format

OAM information fields are self identifying type-length-data entities. Figure 7 depicts the general format of an information field. Each type of information field will be defined in subsequent subclauses.



NOTE 1 – Information field type values are defined in 7.2.5.1.

NOTE 2 – Length includes type, length, and data subfields.

Figure 7/X.151 – OAM information field format

7.2.5.1 IF-type field values

The values for the IF-type field of the OAM information field are defined in Table 3.

Table 3/X.151 – Information field type values

Information field type value	Usage	References
0x01	Capabilities	7.3.1.1
0x02	Frame transfer delay	7.3.1.2
0x03	Frame transfer delay results	7.3.1.3
0x04	Frame delivery ratio sync	7.3.1.4
0x05	Frame delivery ratio results	7.3.1.5
0x06	Data delivery ratio sync	7.3.1.6
0x07	Data delivery ratio results	7.3.1.7
0x08	Non-latching loopback	7.3.1.8
0x09	Latching loopback	7.3.1.9
0x0A	Diagnostic indication	7.3.1.10
0xB	Full source address	7.3.1.11
0xFE	Opaque	7.3.1.12
0xFF	Pad	7.3.1.13

7.2.5.2 Information field length

The length field of an information field includes the type, length and data fields. The value of this field **must** be in the range of 2 through 255 inclusive.

7.3 OAM information fields

An OAM message includes one or more information fields.

7.3.1 Per type formats of information fields

The formats and values of the data field of the OAM information field are dependent upon the information field type.

7.3.1.1 Capabilities information field

The capabilities information field is used to advertise a willingness to participate in OAM functions to other OAM devices within the administrative domain. The format of this field is shown in Figure 8.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	0	0	1	
Length								2
x	x	x	x	x	x	x	x	
Capability #1 (Notes 1 and 2)								3
Capability #N								3 + N

NOTE 1 – Capability field values are multi-octet with the high-order bit used to indicate extension of this capability (high order bit=1 indicates another octet follows for this capability), and are defined in Table 4.

NOTE 2 – The capabilities IF must include the Hello message capability. All other capabilities are optional.

Figure 8/X.151 – Capabilities information field format

Table 4/X.151 – Capability information field type values

Capability field value	Length	Usage
0x01 (see Figure 9)	5-octet	Hello message (Note 1)
0x02	1-octet	Supports frame transfer delay
0x03 (see Figure 9)	5-octet	Supports frame delivery ratio
0x04 (see Figure 9)	5-octet	Supports data delivery ratio
0x05	1-octet	Supports latching loopback
0x06	1-octet	Supports non-latching loopback

The single octet capabilities are formatted using an 8-bit value of the capability from Table 4.

The Hello, frame delivery ratio, and data delivery ratio capabilities use a multi-octet format, which provides a maximum-time capability value. The format for these is shown in Figure 9.

Bits								Octet
8	7	6	5	4	3	2	1	
EA	Capability type							1
1	x	x	x	x	x	x	x	
EA	Capability value (high order bits)							2
1	x	x	x	x	x	x	x	
EA	Capability value (mid-h order bits)							3
1	x	x	x	x	x	x	x	
EA	Capability value (mid-l order bits)							4
1	x	x	x	x	x	x	x	
EA	Capability value (low order bits)							5
0	x	x	x	x	x	x	x	

Figure 9/X.151 – Multi-octet capability format

7.3.1.1.1 Hello message capability

The Hello capability uses a 5-octet extended format supporting a 28-bit value. This value indicates the time (in milliseconds) that the transmitting FROMP advertises as the recommended expiration value of the `TIMER_HELLO_RX` timer.

7.3.1.1.2 Supports FDR capability

The supports FDR capability uses a 5-octet extended format capability supporting a 28-bit value. This value, in milliseconds, represents the maximum amount of time that may expire before any of the transmitting FROMP FDR counters (either its Tx and Rx counters) can cycle.

7.3.1.1.3 Supports DDR capability

The supports DDR capability uses a 5-octet extended format capability supporting a 28-bit value. This value, in milliseconds, represents the maximum amount of time that may expire before any of the transmitting FROMP DDR counters (either its Tx and Rx counters) can cycle.

7.3.1.2 Frame transfer delay information field

The frame transfer delay information field is used to measure Frame Transfer Delay (FTD). The format for this information field is shown in Figure 10.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	0	1	0	
Length								2
0	0	0	0	x	1	1	0	
Initiator TX time-stamp (Note 1)								3
Receiver RX time-stamp (Note 2)								7
Receiver TX time-stamp (Note 2)								11

NOTE 1 – Time-stamp fields shall be 4 octets in length and represent milliseconds. The value is assumed to be of local significance only.

NOTE 2 – These fields are only present in response to an FTD message. The length of the information field (1110 or 0110) is used to determine if this is the request or response.

Figure 10/X.151 – Frame transfer delay information field format

7.3.1.3 Frame transfer delay results information field

The frame transfer delay results information field is used to return the result of a FTD round-trip measurement. The format for this information field is shown in Figure 11.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	0	1	1	
Length								2
0	0	0	0	0	1	1	0	
Calculated result (Note)								3

NOTE – Calculated result is a 4-octet value in milliseconds representing the ONE-WAY FTD determined by a dividing in half the results of the round-trip test measurement initiated by the transmitter of this message.

Figure 11/X.151 – Frame transfer delay results information field format

7.3.1.4 Frame delivery ratio sync information field

The frame delivery ratio sync information field is used to determine the Frame Delivery Ratio (FDR). The format for this information field is shown in Figure 12.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	1	0	0	
Length								2
0	0	0	0	1	1	1	0	
<i>FramesOffered</i> _{Committed}								3
<i>FramesOffered</i> _{Excess} (See Note 1)								7
VC Time (See Note 2)								11

NOTE 1 – Does not include frames in CIR or in excess of CIR + Excess Burst.

NOTE 2 – 4-octet value indicating an approximate time offset (in ms) relative to the counters. This value must increase in successive polls. Set to zero by initiator to indicate a restart condition. See 8.4.4.

Figure 12/X.151 – Frame delivery ratio sync information field format

7.3.1.5 Frame delivery ratio results information field

The frame delivery ratio results information field is used to return the result of a FDR measurement. The format for this information field is shown in Figure 13.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	1	0	1	
Length								2
0	0	0	1	0	0	1	0	
Δ <i>FramesDelivered</i> _{Committed} (Note 1)								3
Δ <i>FramesDelivered</i> _{Excess} (Notes 1 and 2)								7
Δ <i>FramesLost</i> _{Committed} (Note 1)								11
Δ <i>FramesLost</i> _{Excess} (Notes 1 and 2)								15

NOTE 1 – These fields are 4 octets each. They are used to deliver the results of a frame delivery measurement in the reverse direction.

NOTE 2 – Does not include frames within CIR or in excess of CIR + Excess Burst.

Figure 13/X.151 – Frame delivery ratio results information field format

7.3.1.6 Data delivery ratio sync information field

The data delivery ratio sync information field is used to determine the Data Delivery Ratio (DDR). The format for this information field is shown in Figure 14.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	1	1	0	
Length								2
0	0	0	0	1	1	1	0	
<i>DataOffered_{Committed}</i>								3
<i>DataOffered_{Excess}</i> (Note 1)								7
VC Time (Note 2)								11

NOTE 1 – Does not include frames within CIR or in excess of CIR + Excess Burst.

NOTE 2 – 4-octet value indicating an approximate time offset (in ms) related to the counters. This value must increase in successive polls. Set to zero by initiator to indicate a restart condition. See 8.4.5.

Figure 14/X.151 – Data delivery ratio sync information field format

7.3.1.7 Data delivery ratio results information field

The data delivery ratio results information field is used to return the result of a DDR measurement. The format for this information field is shown in Figure 15.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	0	1	1	1	
Length								2
0	0	0	1	0	0	1	0	
$\Delta DataDelivered_{Committed}$ (Note 1)								3
$\Delta DataDelivered_{Excess}$ (Notes 1 and 2)								7
$\Delta DataLost_{Committed}$ (Note 1)								11
$\Delta DataLost_{Excess}$ (Notes 1 and 2)								15

NOTE 1 – These fields are 4 octets each. They are used to deliver the results of a data delivery measurement in the reverse direction.

NOTE 2 – Does not include frames within CIR or in excess of CIR + Excess Burst.

Figure 15/X.151 – Data delivery ratio results information field format

7.3.1.8 Non-latching loopback information field

The non-latching loopback information field is used to perform minimally intrusive operational diagnostic actions. The format for this information field is shown in Figure 16.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	1	0	0	0	
Length								2
x	x	x	x	x	x	x	x	
Non-Latching Loopback Code (Note 1)								3
Option Data (Note 2)								5

NOTE 1 – Non-latching code values are defined in Table 5.

NOTE 2 – Length of this field may be determined from length of the IF. Option data **may** be present and content is not subject to standardization.

Figure 16/X.151 – Non-latching loopback information field format

Table 5/X.151 – Non-latching loopback code values

Command value	Usage
0x01	Non-latched loop frame request
0x02	Non-latched loop frame response

7.3.1.9 Latching loopback information field

The latching loopback information field is used to perform service affecting operational diagnostic actions. The format for this information field is shown in Figure 17.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	1	0	0	1	
Length								2
0	0	0	0	0	0	1	1	
Latching loopback code (Note)								3

NOTE 1 – 1-octet value. Latching loopback code values are defined in Table 6.

Figure 17/X.151 – Latching loopback information field format

Table 6/X.151 – Latched loopback code values

Command value	Usage
0x01	Latched Loop Enable Request
0x02	Latched Loop Disable Request
0xFF	Latched Loop Denied

7.3.1.10 Diagnostic indication information field

The diagnostic indication information field is used to convey operational information to other OAM devices. The format for this information field is shown in Figure 18.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	1	0	1	0	
Length								2
x	x	x	x	x	x	x	x	
Event type (Note 1)								3
Event location (Note 2)								4

NOTE 1 – See Table 7.

NOTE 2 – Length and content of this field is not subject to standardization.

Figure 18/X.151 – Diagnostic indication information field format

Table 7/X.151 – Event types for diagnostic indication

Event type value	Usage
0x00	VC latching loopback enabled
0x01	VC latching loopback disabled
0x02	Phy down
0x03	Phy up

7.3.1.11 Full source address information field

The full source address information field **may** be used by an OAM device to advertise a more complete identification of the device. This is for use by higher layer management. The format for this information field is shown in Figure 19.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								1
0	0	0	0	1	0	1	1	
Length								2
x	x	x	x	x	x	x	x	
Address type (Note)								3
Address information								4

NOTE – Address type values are shown in Table 8.

Figure 19/X.151 – Full source address information field

Table 8/X.151 – Address type values

Address type value	Usage
0x01	Clear text (Null terminated string)
0xCC	IPv4 address (4-octet)
0xFD	AESA identified per ITU-T Rec. X.36
0xFE	E.164 address per ITU-T Rec. X.36
0xFF	X.121 address per ITU-T Rec. X.36

7.3.1.12 Opaque information field

The opaque information field allows for vendor-specific extensions to the OAM protocol. An implementation receiving an opaque information field **may** choose to process or ignore this information field based upon the organizationally unique identifier (OUI) contained in the field. The OUI information field **may** be repeated within an OAM message. The format for this information field is shown in Figure 20.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								
1	1	1	1	1	1	1	0	1
Length								
x	x	x	x	x	x	x	x	2
Organizationally Unique Identifier (OUI) (Note 1)								3
Subcode (Note 2)								6
Vendor-specific data (Note 3)								7

NOTE 1 – OUIs are assigned by IEEE. Bit-8 is the most significant bit.

NOTE 2 – Content of subcode field is not subject to standardization.

NOTE 3 – Length and contents of vendor-specific data field are not subject to standardization.

Figure 20/X.151 – Opaque information field format

7.3.1.13 Pad information field

The pad information field **may** be used to create an OAM message with a specific length. The pad information field **may** be repeated within an OAM message as needed. The format for this information field is shown in Figure 21.

Bits								Octet
8	7	6	5	4	3	2	1	
Type								
1	1	1	1	1	1	1	1	1
Length (Note 1)								
x	x	x	x	x	x	x	x	2
Padding (Note 2)								3

NOTE 1 – Length may be from 2-255.

NOTE 2 – Content of the padding field is not subject to standardization.

Figure 21/X.151 – Pad information field format

8 OAM procedures

This clause describes a set of rules for processing OAM messages that use the formats described in clause 7.

Clause 8.1 describes rules for the encoding and decoding of messages.

Clause 8.2 provides the general rules for the processing of OAM messages.

Procedures to discover peer FROMPs, and advertise capabilities, via the Hello message are covered in 8.3.

Service level measurement procedures using the service verification message are detailed in 8.4.

Procedures for the non-latching and latching loopback messages are covered in 8.5 and 8.6.

Procedures for the diagnostic indications message are covered in 8.7.

8.1 Message encoding/decoding rules

Implementations of this Recommendation **should** process the decoding of messages described in clause 7 using the following general rules:

- Improperities in the message header, such as an ill-formed address or unknown message type, **should** cause the entire message to be discarded.
- An improperly formed information field **should** be ignored along with the remainder of the message, and the remainder of the message processed. One example would be any information field with a length of zero or one.
- A properly formed, but unknown, information field **should** be ignored and the remainder of the message processed.
- A properly formed information field with an unexpected length **should** be ignored and the remainder of the message processed.
- If the last information field is not complete, this field should be ignored, however, the remainder of the message **may** be processed.

OAM messages passing through a FROMP are not subject to information field decoding and **should** be forwarded intact.

8.1.1 Order of transmission

Throughout this Recommendation multi-octet values **shall** be transmitted from most significant byte to least significant byte (MSB) order.

When bits are depicted in the formats, bit-8 is the most significant bit.

8.1.2 Order of information fields

Information fields within an OAM message **must** be presented in ascending order of information field type values. For example, the capabilities information field, when present, **must** be the first information field present in the message. Similarly, the pad information field **must** be the last element when present. Only the opaque and pad information fields are allowed to be repeated within an OAM message.

8.1.3 Usage of information fields

Each OAM message **must** include at least one information field. The maximum number of information fields is limited by MTU size.

Information fields are included in an OAM message dependent upon the message type indicated in the OAM header. Table 9 defines information fields that **may** be included for each message type. Fields marked N/A may not be used in a message of the indicated message type. A message containing an information field that is of an unknown information field type, or containing an information field that is not allowed for the indicated message type, will be ignored without affecting the processing of subsequent information fields.

Table 9/X.151 – Information fields by message type

IF type value	Usage	Hello message	Service verification message	Latching loopback message	Non-latching loopback message	Diagnostic indication message
0x01	Capabilities	Mandatory	N/A	N/A	N/A	N/A
0x02	Frame transfer delay	N/A	Optional	N/A	N/A	N/A
0x03	Frame transfer delay results	N/A	Optional	N/A	N/A	N/A
0x04	Frame delivery ratio sync	N/A	Optional	N/A	N/A	N/A
0x05	Frame delivery ratio results	N/A	Optional	N/A	N/A	N/A
0x06	Data delivery ratio sync	N/A	Optional	N/A	N/A	N/A
0x07	Data delivery ratio results	N/A	Optional	N/A	N/A	N/A
0x08	Non-latching loopback	N/A	N/A	N/A	Mandatory	N/A
0x09	Latching loopback	N/A	N/A	Mandatory	N/A	N/A
0x0A	Diagnostic indication	N/A	N/A	N/A	N/A	Mandatory
0x0B	Full source address	Optional	N/A	N/A	N/A	N/A
0xFE	Opaque	Optional	Optional	Optional	Optional	Optional
0xFF	Pad	Optional	Optional	Optional	Optional	Optional

8.1.4 Counters and counter wrap

These procedures support the use of various fixed length counters that will wrap (roll over to zero). Implementations of these procedures **must** support normal counter-wrapping to occur. Computations using these counters take into consideration the maximum value, and upon receiving a lower value in a subsequent message assume the counter has wrapped once.

8.2 General message processing

General rules for the transmission, reception and forwarding of OAM messages are described in this clause.

8.2.1 Transmission of messages

A FROMP generating an OAM message **shall** always provide valid domain identification, source location identifier, and destination location identifier data in the OAM message header.

The domain identification **shall** uniquely identify all administrations on the virtual circuit. Service Providers **should** use their X.121 or E.164 network identifiers. The domain identification **must** be one of the domains for which the transmitting OAM device is a member. OAM messages **must not** use the "all domain broadcast" domain identification plan.

The source location identifier **must** be unique within this domain on this VC. The source location identifier used by a FROMP **should** be the same on a given VC for all domains.

The destination location identifier can either be the global destination identifier (see 7.2.4), or it can be the source location identifier received in a Hello message from another device (see 8.3). The global destination address is used only for the Hello message type.

8.2.2 Reception and forwarding of messages

OAM messages arriving at an interface of a FROMP may be discarded, processed, and/or forwarded according to the rules in this clause. Figure I.1 provides an example flow chart depicting the decision-making logic that can be used.

A FROMP **must** distinguish between arriving messages with domain identification matching a domain of which the FROMP is a member, and those that are not. These messages will be referred to as being "in the same domain" and "from a foreign domain" respectively.

8.2.2.1 Arriving OAM message from a foreign domain

A FROMP must forward (local conditions permitting) any messages that do not match its domain identification.

8.2.2.2 Arriving OAM messages from same domain

Messages arriving at an interface of a FROMP that match its domain identification are processed according to the rules of this clause. In some cases, the messages are treated differently depending upon whether this FROMP terminates the administrative domain associated with this message.

8.2.2.2.1 Duplicate location identifier detection

At any FROMP, a message that contains a domain identification and source location identifier that match those of the receiving entity shall be discarded. A FROMP detecting this condition should send an indication of the conflict to the network management layer.

8.2.2.2.2 Arriving at a non-boundary device

A FROMP that does not terminate a domain boundary **must**:

- Receive for further processing, and not forward, messages with the same domain identification and a matching destination location identifier.
- Receive for further processing, and forward (subject to congestion), messages with the same domain identification and the broadcast destination identifier.
- Forward (subject to congestion), without receiving for further processing, messages with the same domain identification and a destination location identifier that is neither matching nor the broadcast identifier.

8.2.2.2.3 Arriving at a boundary device

A FROMP that does terminate a domain boundary **must**:

- Discard without processing, or forwarding, all messages with the same domain identification that arrive on an interface that is outside the domain boundary. For example, in Figure 3, for a device at location B₁, messages arriving from the direction of location A₁ are discarded if Domain B is identified. The FROMP **may** send an indication of the conflict to the device's network management layer.
- Receive for further processing, and not forward, messages with the same domain and a matching destination location identifier or broadcast location identifier arriving on an interface that is inside the domain boundary.
- Discard without processing, or forwarding, all messages with the same domain identification and a destination identifier that is neither matching nor the broadcast identifier arriving on an interface that is inside the domain boundary.

8.2.3 Timers

A number of timers are defined in these procedures. These timers are used per Domain/Interface in some cases, and domain/interface/peer in others. Table 10 summarizes these timers, their ranges and defaults.

Table 10/X.151 – OAM timers

Name	Purpose	Range	Default
TIMER_HELLO_TX	Send Hello message (Discovery)	15-3600 seconds	900 seconds
TIMER_HELLO_RX	Detect lost peer (Discovery)	60-14400 seconds	3200 seconds
TIMER_SLV	Initiate SLV measurement(s)	15-3600 seconds	900 seconds

8.3 Hello message processing (device discovery)

Peer FROMPs are discovered when a Hello message is received on the frame relay connection from another OAM device in the same administrative domain. The Hello message contains information about the peer FROMP's capabilities and are transmitted periodically based upon the TIMER_HELLO_TX timer.

If a FROMP is in the middle of an administrative domain (not a boundary device), two Hello messages are transmitted; one message towards each VC endpoint. If a FROMP is at the administrative boundary, the Hello messages will only be transmitted on the interface within the domain. Each Hello message applies to a single domain as encoded in the domain identification field of the message header. If a FROMP supports multiple domains (e.g., Figure 22 C₁/F₁) a separate message **must** be generated for each domain. A device **may** advertise a different capability set for each domain.

The following functions are provided by the discovery procedure:

- Association of a FROMP with one or more administrative domains;
- Association of a FROMP with a specific location identifier for an administrative domain;
- Advertisement of OAM capabilities supported by the device; and
- Support for vendor extensions via the opaque field.

Figure 22 illustrates transmission of the Hello message from a number of hypothetical FROMPs located on the path of a single virtual connection.

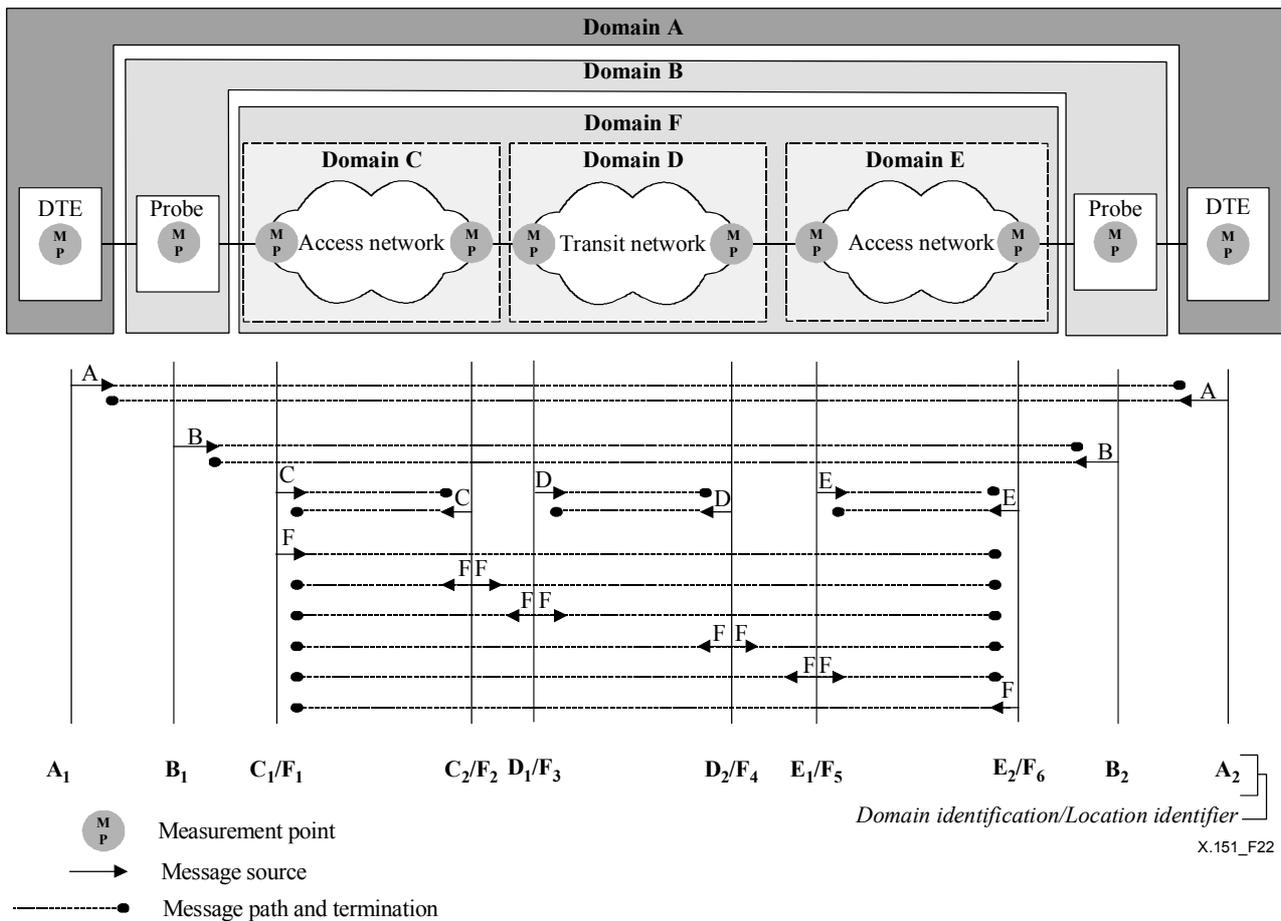


Figure 22/X.151 – Example of Hello messages on a VC with multiple administrative domains

Appendix II.1 provides an example of message flows for Hello messages between two peer FROMPs in the same domain.

8.3.1 Sending the Hello message

For each virtual circuit for each domain that this FROMP is participating in, the following procedures apply. Implementations are encouraged to use techniques that prevent bursts of Hello messages from being transmitted.

8.3.1.1 Connection initialization

A FROMP **may** initiate the discovery process upon establishment of the connection. In the case of PVCs, establishment is indicated when Q.933 signalling status messages report the virtual connection as "active". If the FROMP is positioned at the network-to-network interface then both networks need to report the virtual connection as "active" for the connection to be considered established. In the case of SVCs, establishment is indicated when the Q.933 CONNECT message is received.

Upon initiating the discovery process, the FROMP transmits a Hello message. The message **shall** be sent with a destination location identifier for the global destination. A FROMP at a domain boundary in a network **may not** send the Hello message on a segment of the connection that is not part of the domain. For example, location D₂ in Figure 22 sends a Hello message for Domain D towards location D₁ but never towards location E₁.

Capabilities advertised via the capabilities information field **must** remain available for the duration of the frame relay connection. Additional capabilities **may** be added in subsequent Hello messages (for example due to changes initiated by a higher layer management operation). Once added, the new capabilities **must** remain available for the duration of the frame relay connection. In the case of multi-octet time intervals advertised in the capabilities information field, the interval **may not** change in subsequent Hello messages.

8.3.1.2 Periodic transmission interval

All FROMPs **shall** transmit the Hello message periodically. Upon transmitting a Hello message for a domain on an interface, the device **shall** set a timer, `TIMER_HELLO_TX`.

Transmission of the Hello message **may** be suspended when the data link connection is not operational. Examples of causes include:

- a failure of the link integrity verification mechanism;
- the clearing of the "active" bit;
- the setting of the "delete" bit;
- the absence of the data link connection information element.

Transmission of the Hello message **should** resume upon connection initialization as described in 8.3.1.1.

8.3.2 Processing the received Hello message

The received Hello message shall be compared with previously recorded hello messages from this peer on this VC. The timer, `TIMER_HELLO_RX`, is (re)set for this peer. The peer provides a recommended value for this timer in the supports Hello capability.

8.3.2.1 Discovery of a new peer

Receiving a valid Hello message from a new peer device enables this device to send OAM messages of message types other than Hello directed towards this new peer. The capabilities listed in this Hello message shall be maintained and honoured. OAM communication to this peer **may** be initiated immediately upon receipt of a single Hello message from the peer.

8.3.2.2 Previously recorded peer

Upon receiving a valid Hello message from an existing peer, the contents of the capabilities information field **shall** be examined for new and/or improved capabilities.

8.3.3 `TIMER_HELLO_RX` expiration

A time out algorithm for detecting that an OAM device is no longer advertising its presence and willingness to participate in OAM with the Hello message is recommended. It is further suggested that such an algorithm allow for implementations that use variable logic for their `TIMER_HELLO_TX` value.

Upon detecting such a timeout expiration condition, procedures to initiate service level verification measurements **should** be discontinued.

8.4 Service level verification message processing

Service level verification and segment-oriented quality of service measurement is performed by use of the service verification message. In most cases, a measurement requires multiple messages to be exchanged between two OAM peer devices. In some cases, these measurements measure a service parameter in one direction, and a separate independent measurement **may** be needed in the reverse direction.

There are three service measurements supported by the service verification message:

- Frame transfer delay;
- Frame delivery ratio;
- Data delivery ratio.

The three measurements are implemented with independent information fields. These measurements are independent of each other, although in many cases they will be combined in a single message.

Appendices II.2 and II.3 provide an example of message flows for FTD and FDR/DDR.

8.4.1 Sending the service verification message

The service verification message **must** be transmitted only using a specific (non-broadcast) destination location. A FROMP **must** receive at least one Hello message from a peer prior to transmission of a service verification message to this location.

8.4.1.1 Periodic transmission interval for measurement initiations

Each type of service measurement **may** use an independent timer (designated `TIMER_SLV_*`), or share a single timer (designated `TIMER_SLV`). At the expiration of any `TIMER_SLV`, the FROMP **may** send the service verification message.

The value of any `TIMER_SLV` is not subject to standardization. A FROMP **must** take the received maximum interval from a peer device into account in setting its `TIMER_SLV`. The recommended default interval for `TIMER_SLV` is 900 seconds.

8.4.2 Processing the received service verification message

Processing of the received message is entirely dependent upon the information fields present. The presence of these information fields indicates which function(s) are to be performed. Clauses 8.4.3, 8.4.4 and 8.4.5 describe procedures based upon the function being performed.

8.4.3 Procedures for delay measurement

In this procedure, a round-trip delay measurement is made. This measurement is divided in half to obtain the one-way FTD measurement.

A frame transfer delay measurement requires a two-way exchange between initiator and receiver FROMPs. The initiator begins the measurement by sending a message with the frame transfer delay information field; the receiver loops the message back after filling in additional time-stamps. Optionally, the initiator **may** then deliver a copy of the results back to the receiver using the frame transfer delay results information field.

This procedure uses the frame transfer delay IF, the frame transfer results IF, and the pad IF. An example of message flows between the initiator and receiver devices is shown in Figure II.2.

8.4.3.1 Delay initiation

On the initiation of a delay measurement, the initiator device transmits the frame transfer delay IF using the short form (6 octets). The initiator **shall** fill in the initiator TX time-stamp with a value representing the time the opening bit of the frame will begin transmission.

8.4.3.2 Delay turnaround

Upon receiving a frame transfer delay IF of the short form, the receiver device responds to the initiator with the frame transfer delay IF long form (12 octets). The responder **shall** copy the initiator Tx time-stamp, fill in the responder Rx time-stamp with a value representing the arrival time of the closing bit of the frame, and fill in the responder Tx time-stamp with a value representing the time the opening bit of the frame will begin transmission. This response **shall** be

sent in an OAM message padded to the same length as was received. The pad information field is available to be used for this purpose.

8.4.3.3 Delay measurement

Upon receiving a frame transfer delay IF of the long form, the initiator device **shall** record a time-stamp with a value representing the arrival time of the closing bit of the frame. Calculation of FTD is performed using the following equation:

$$FTD = ((Initiator_Rx - Initiator_Tx) - (Responder_Tx - Responder_Rx))/2$$

8.4.3.4 Delivery of delay results

Dependent upon provisioning, the initiator device **may** forward the calculated one-way FTD results to the receiver device using the frame transfer delay results IF. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

8.4.3.5 Error handling

A lost or damaged FTD request or response message can result in a missed measurement period. Implementations **may** optionally time out and retransmit to recover the period.

8.4.3.6 Procedures for the estimation of frame delay jitter

Clause 5.2/X.144 defines Frame Delay Jitter (FDJ) as the maximum frame transfer delay (FTD_{max}) minus the minimum frame transfer delay (FTD_{min}) during a given measurement interval, consisting of a statistically significant number of delay measurements (N).

$$FDJ = FTD_{max} - FTD_{min}$$

where:

FTD_{max} is the maximum FTD recorded during a measurement interval of N delay measurements;

FTD_{min} is the minimum FTD recorded during a measurement interval of N delay measurements;

N is the number of FTD measurements made to give a statistically significant representation of the FTD performance. N must be chosen to be at least 1000 (see Note).

NOTE – This number of 1000 observations will ensure that the 99.5 percentile of delay is observed at least 99% of the time. The suggested measurement interval is five (5) minutes. It is desirable that the observations be distributed uniformly across the measurement interval.

Accordingly, a running estimate of FDJ can be obtained from a statistical analysis of the collected values of a statistically significant number of transfer delay measurements.

8.4.4 Procedures for frame delivery ratio measurement

In this procedure, a one-way measurement is made of the delivery ratio from the initiator to the receiver. This measurement satisfies the requirements for calculating FDR, FDRc and FDRc.

A complete frame delivery ratio measurement requires multiple exchanges between the initiator and receiver. The beginning of a measurement session requires the initiator to send a sync indication. Measurements **may** then be made by the initiator sending a second FDR Sync IF message to the receiver. This creates a one-way measurement of the parameter. The receiver **may** send a copy of the results back to the initiator by using the frame delivery results information field. An independent measurement session **may** also be established in the reverse direction.

This procedure uses the frame delivery ratio sync IF, and the frame delivery results IF. An example of message flows between the initiator and receiver devices is shown in Figure II.3. An example of a method to perform this measurement is shown in Appendix III.

8.4.4.1 Frame delivery ratio initiation

The frame delivery ratio sync IF is used to initialize (or reinitialize) an FDR measurement session.

The initiator of this message shall fill in the VC time (in milliseconds) to ensure that the receiver interprets the message to indicate a(n) (re)initialization. A VC time of zero is used to indicate initiation or re-initialization.

The initiator of this message shall also fill in the current counters for this VC (*FramesOffered_{Committed}* and *FramesOffered_{Excess}*) prior to this message being transmitted. OAM messages **must** be included in these frame counters.

When a frame delivery ratio sync IF is received with the VC time value set to zero, or less than the previous received value (taking into account normal counter-wrapping), the receiver **shall** terminate any previous session and restart a new session. A FROMP receiving this information field (regardless of the VC time indicated) **shall** record the receiver frame counts representing the counters for this VC (*FramesReceived_{Committed}* and *FramesReceived_{Excess}*) as they were prior to the reception of this frame.

8.4.4.2 Frame delivery ratio measurement

The frame delivery ratio sync IF is also used to complete a one-way measurement of the ratio of frames delivered to frames offered. The initiator device of this message shall fill in the current counters for this VC (*FramesOffered_{Committed}* and *FramesOffered_{Excess}*) prior to this message being transmitted. When wrapping of the VC time occurs, the initiator **shall** ensure that a value of zero is not sent.

A FROMP receiving the frame delivery ratio sync IF **shall** record the receiver frame counts representing the counters for this VC (*FramesReceived_{Committed}* and *FramesReceived_{Excess}*) as they were prior to the reception of this frame. The value of the VC time **shall** be inspected for indications of a restart as described in the previous clause.

The receiving device **shall** determine if the recorded maximum interval has been exceeded.

- If the interval has been exceeded, the device **shall not** use the previous counters to calculate the FDR for the interval terminated by this message. The counters from this poll **shall** be stored such that the next poll in this measurement session will be valid if it is received within the allowable interval.
- If the interval has not been exceeded, the device **shall** use these counters to calculate the FDRs for the interval. FDRs for the receive direction are calculated using the following formulae:

$$\Delta \text{FramesOffered}_{\text{Committed}} = \text{FramesOffered}_{\text{Committed}2} - \text{FramesOffered}_{\text{Committed}1}$$

$$\Delta \text{FramesOffered}_{\text{Excess}} = \text{FramesOffered}_{\text{Excess}2} - \text{FramesOffered}_{\text{Excess}1}$$

$$\Delta \text{FramesDelivered}_{\text{Committed}} = \text{FramesReceived}_{\text{Committed}2} - \text{FramesReceived}_{\text{Committed}1}$$

$$\Delta \text{FramesDelivered}_{\text{Excess}} = \text{FramesReceived}_{\text{Excess}2} - \text{FramesReceived}_{\text{Excess}1}$$

$$\Delta \text{FramesLost}_{\text{Committed}} = \Delta \text{FramesOffered}_{\text{Committed}} - \Delta \text{FramesDelivered}_{\text{Committed}}$$

$$\Delta \text{FramesLost}_{\text{Excess}} = \Delta \text{FramesOffered}_{\text{Excess}} - \Delta \text{FramesDelivered}_{\text{Excess}}$$

$$\text{FDR}_{\text{C}} = \Delta \text{FramesDelivered}_{\text{Committed}} / \Delta \text{FramesOffered}_{\text{Committed}}$$

$$\text{FDR}_{\text{E}} = \Delta \text{FramesDelivered}_{\text{Excess}} / \Delta \text{FramesOffered}_{\text{Excess}}$$

$$FDR = \frac{(\Delta FramesDelivered_{Committed} + \Delta FramesDelivered_{Excess})}{(\Delta FramesOffered_{Committed} + \Delta FramesOffered_{Excess})}$$

The device **shall** record the counters for use by the next "FDR Sync" message.

8.4.4.3 Delivery of frame delivery ratio results

Dependent upon provisioning, the receiver device **may** forward the calculated one-way FDR results to the initiator device using the frame delivery ratio results IF. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

8.4.4.4 FDR error handling

A lost or damaged FDR sync message **may** result in one or more missed measurement intervals. If the maximum interval for counter-wrap (advertised by the peer in the capabilities information field) does not expire prior to the next successful FDR sync message, this next complete measurement will span the period between the two received messages. If the maximum interval for counter-wrap occurs, the next successful FDR sync message is treated as if it were a restart. In this case, the prior interval(s) are lost and FDR results **shall not** be sent.

8.4.4.5 Frame loss ratio calculation

It is common for Frame Loss Ratio (FLR) as defined in ITU-T Rec. X.144 to be used as a performance metric. An estimate of the FLR can be readily calculated from the values (frame counts) in the frame delivery ratio results information field.

Clause 5.3/X.144 defines the user information frame loss ratio (FLR) as:

$$FLR = \frac{F_L}{F_S + F_L + F_E}$$

where, in a specified population:

F_S is the total number of successfully transferred frame outcomes;

F_L is the total number of lost frame outcomes; and

F_E is the total number of residually errored frame outcomes.

Assuming $F_E = 0$

$$+F_L = (FramesLost_{Committed} + FramesLost_{Excess})$$

$$F_S = (FramesDelivered_{Committed} + FramesDelivered_{Excess})$$

$$FLR = \frac{(FramesLost_{Committed} + FramesLost_{Excess})}{(FramesDelivered_{Committed} + FrameDelivered_{Excess}) + (FramesLost_{Committed} + FramesLost_{Excess})}$$

8.4.5 Procedures for data delivery ratio measurement

In this procedure, a one-way measurement is made of the delivery ratio from the initiator to the receiver. This measurement satisfies the requirements for calculating DDR, DDRc, and DDRc.

A complete data delivery ratio measurement requires multiple exchanges between the initiator and receiver. The beginning of a measurement session requires the initiator to send a sync indication. Measurements **may** then be made by the initiator sending a second DDR sync IF message to the receiver. This creates a one-way measurement of the parameter. The receiver **may** send a copy of the results back to the initiator by using the frame delivery results information field. An independent measurement session **may** also be established in the reverse direction.

This procedure uses the data delivery ratio sync IF, and the data delivery results IF. An example of message flows between the initiator and receiver devices is shown in Figure II.3. An example of a method to perform this measurement is shown in Appendix III.

8.4.5.1 Data delivery ratio initiation

The data delivery ratio sync IF is used to initialize (or re-initialize) a DDR measurement session.

The initiator of this message shall fill in the VC time (in milliseconds) to ensure that the receiver interprets the message to indicate a(n) (re)initialization. A VC time of zero is used to indicate initiation or re-initialization.

The initiator of this message shall also fill in the current counters for this VC (*DataOffered_{Committed}* and *DataOffered_{Excess}*) prior to this message being transmitted. OAM messages **must** be included in these data counters.

When a data delivery ratio sync IF is received with the VC time set to zero, or a value less than the previous received value from the initiator, the receiver **shall** terminate any previous session and restart a new session. A FROMP receiving this information field (regardless of the VC time indicated) **shall** record the receiver frame counts representing the counters for this VC (*DataReceived_{Committed}* and *DataReceived_{Excess}*) as they were prior to the reception of this frame.

8.4.5.2 Data delivery ratio measurement

The data delivery ratio sync IF is also used to complete a one-way measurement of the ratio of octets delivered to octets offered. The initiator device of this message shall fill in the current counters for this VC (*DataOffered_{Committed}* and *DataOffered_{Excess}*) prior to this message being transmitted.

A FROMP receiving the data delivery ratio sync IF **shall** record the receiver octet counts representing the counters for this VC (*DataReceived_{Committed}* and *DataReceived_{Excess}*) as they were prior to the reception of this frame. The value of the VC time **shall** be inspected for indications of a restart as described in the previous clause.

The receiving device **shall** determine if the recorded maximum interval has been exceeded.

- If the interval has been exceeded, the device **shall not** use the previous counters to calculate the DDR for the interval terminated by this message. The counters from this poll **shall** be stored such that the next poll in this measurement session will be valid if it is received within the allowable interval.
- If the interval has not been exceeded, the device **shall** use these counters to calculate the DDRs for the interval. DDRs for the receive direction are calculated using the following formulae:

$$\Delta DataOffered_{Committed} = DataOffered_{Committed2} - DataOffered_{Committed1}$$

$$\Delta DataOffered_{Excess} = DataOffered_{Excess2} - DataOffered_{Excess1}$$

$$\Delta DataDelivered_{Committed} = DataReceived_{Committed2} - DataReceived_{Committed1}$$

$$\Delta DataDelivered_{Excess} = DataReceived_{Excess2} - DataReceived_{Excess1}$$

$$\Delta DataLost_{Committed} = \Delta DataOffered_{Committed} - \Delta DataDelivered_{Committed}$$

$$\Delta DataLost_{Excess} = \Delta DataOffered_{Excess} - \Delta DataDelivered_{Excess}$$

$$DDR_C = \Delta DataDelivered_{Committed} / \Delta DataOffered_{Committed}$$

$$DDR_E = \Delta DataDelivered_{Excess} / \Delta DataOffered_{Excess}$$

$$DDR = \frac{(\Delta DataDelivered_{Committed} + \Delta DataDelivered_{Excess})}{(\Delta DataOffered_{Committed} + \Delta DataOffered_{Excess})}$$

The device **shall** record the counters for use by the next "DDR Sync" message.

8.4.5.3 Delivery of data delivery ratio results

Dependent upon provisioning, the receiver device **may** forward the calculated one-way DDR results to the initiator device using the data delivery ratio results IF. Such forwarding **may** be done immediately, or held for inclusion in the next measurement interval.

8.4.5.4 DDR error handling

A lost or damaged DDR sync message **may** result in one or more missed measurement intervals.

- If the maximum interval for counter-wrap (advertised by the peer in the capabilities information field) does not expire prior to the next successful DDR Sync message, this next complete measurement will span the period between the two received messages.
- If the maximum interval for counter-wrap occurs, the next successful DDR sync message is treated as if it were a restart. In this case, the prior interval(s) are lost and DDR results **shall not** be sent.

8.5 Non-latching loopback message processing

Frame relay OAM diagnostics **may** be performed on a segment of a VC between two OAM devices belonging to the same domain. There are two forms of diagnostics supported, a latching VC loopback and a non-latching loopback:

- The latching form is a service maintenance action that will remove the VC from service.
- The non-latching form is used to echo an individual OAM frame without taking the VC out of service.

The non-latching loopback procedures are contained in this clause. The procedures for the latching loopback are in 8.6. Implementations **may** send either form of loopback prior to receiving a Hello message.

The non-latching loopback message causes only the non-latching loop message itself to be looped back to the initiator. An example of messaging between the initiator and the receiver is shown in Figure II.4.

The non-latching loopback message **must** be transmitted using a specific (non-broadcast) destination location.

8.5.1 Initiating the non-latching loopback request

A FROMP initiates a request for a peer device to perform a non-latching loopback by using the non-latching loopback message with the latched loopback code of the non-latching loopback information field set to request. The length and content of this option data is not subject to standardization.

8.5.2 Processing the received non-latching loopback message

A FROMP receiving the non-latching loopback message **must** determine if the message's domain identification indicates membership within one of the domains supported at the receiving location and if the message's destination location indicator indicates this OAM device.

If the message is addressed for this location and the device supports this capability, then the message is processed.

If the non-latching loopback information field indicates a non-latched loopback request, the device **must** accept the request, and respond with a non-latching loopback message of identical length and content, except that:

- 1) The message source and destination locations are reversed.
- 2) The non-latching loopback code of the non-latching loopback information field is set to indicate a response.

If the non-latching loopback information field indicates a non-latched loopback response, the message is terminated.

8.6 Latching loopback message processing

The latched loopback causes all arriving frames on the VC to be looped back towards the transmitter of the latched loopback message. Other VCs passing through this device are not affected. It is a one-way loopback that will not forward received frames further along the VC while the loopback is active. OAM frames shall not pass through the OAM device while the loopback is active, however, OAM frames addressed to this device shall be processed (removing from the looped data when appropriate) and responded to (adding to the looped data). This loopback is shown in Figure 23.

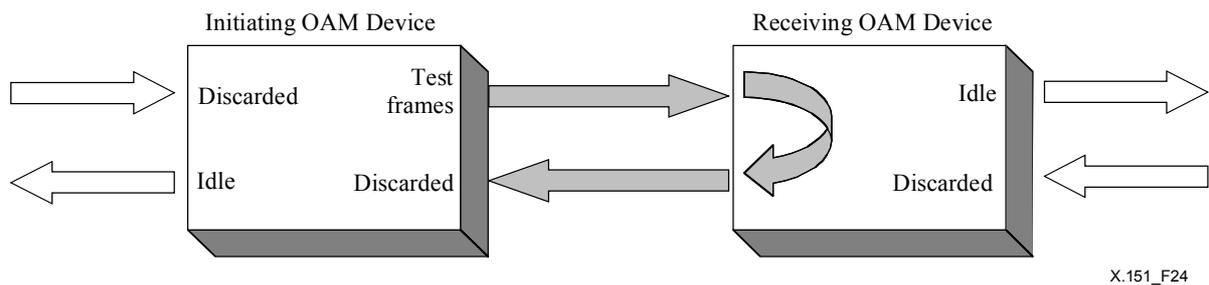


Figure 23/X.151 – VC latched loopback

The latching loopback message **must** be transmitted using a specific (non-broadcast) destination location. An example of messaging between the initiator and receiver is given in Figure II.5.

8.6.1 Initiating the latching loopback request

A FROMP initiates a request for a peer device to perform a latching loopback by using the latching loopback message with the latching loopback information field set to enable.

8.6.2 Processing the received latching loopback request

A FROMP receiving the latching loopback message **must** determine if the message's domain identification indicates membership within one of the domains supported at the receiving location and if the message's location indicator indicates this OAM device. If the message is not addressed for this location, the message **must** be forwarded towards the connection terminus.

If the message is addressed for this location and the device supports this capability, then the message is processed.

If the latching loopback information field indicates a latched loopback enable request, the device **may** either accept the request or reject it. If the request is rejected, the receiver shall respond to the initiator with a latching loopback message and latching loopback information field indicating the rejection.

A VC latched loopback is an intrusive action that will disrupt the flow of data on the VC. If the receiving device also supports the diagnostic indications message, it **must** send a diagnostic indication message in each direction on the affected VC for each domain that it is a member of (see 8.7). Such indications **should** be sent prior to enabling a VC loopback.

If the latching loopback information field indicates a latched loopback disable request, the device **must** accept the request. If the receiving device also supports the diagnostic indications message, it **must** send a diagnostic indication message in each direction on the affected VC for each domain that it is a member of (see 8.7). Such indications **should** be sent after disabling a VC loopback.

8.6.3 Clearing a latched loopback

A FROMP may request a peer to clear a latching loopback condition by issuing a latching loopback message with a latching loopback information field with a disable request. This disable request may be sent by any peer in the domain, and from any direction (not only from the peer that initiated the loopback). The loopback may also be cleared by local management action.

8.7 Diagnostic indication message processing

The diagnostic indication message is optionally used to signal peer FROMPs with indications of traffic affecting conditions. Devices should not rely upon the presence or absence of a diagnostic indication message. The ability of the network to deliver this message may be compromised due to the condition being signalled.

8.7.1 Initiating the diagnostics indication message

A FROMP may send the diagnostics indication message when conditions necessitate. The transmitting device may transmit the message to individual destinations or use the broadcast destination address for a given domain. The message **shall** use the diagnostic indication information field with the appropriate indication. PHY_UP and PHY_DOWN **may** be used to notify peer FROMPs of a service affecting change detected at the physical interface.

8.7.2 Processing the received diagnostic indication message

A FROMP receiving the diagnostic indication message **must** determine if the message's domain identification indicates membership within one of the domains supported at the receiving location and if the message's destination location indicator indicates this OAM device (or the broadcast address).

If the message is addressed for this location and the device supports this capability, then the message is processed.

The actions to be taken upon reception of the diagnostic indication message are not subject to standardization.

8.8 Network applications of loopback

Loopback frames can be used to locate a fault by identifying working and non-working segments.

8.8.1 Fault isolation

The loopback capability supports the following network applications as shown in Figure 24.

- a) End-to-end loopback: An FR loopback frame is inserted by an FR endpoint, and looped back by the corresponding FR endpoint.
- b) Access line loopback: An FR loopback frame is inserted by the customer or the network, and looped back by the first frame relay node in the network or customer equipment respectively.
- c) Inter-domain loopback: An FR loopback frame is inserted by one network operator, and looped back by the first frame relay node (at the FR level) in an adjacent network operator domain.
- d) Network-to-endpoint loopback: An FR frame is inserted by one network operator, and looped back by the FR endpoint in another domain.
- e) Intra-domain loopback: An FR loopback frame is inserted by an FR connecting point, and looped back by another FR connecting point.

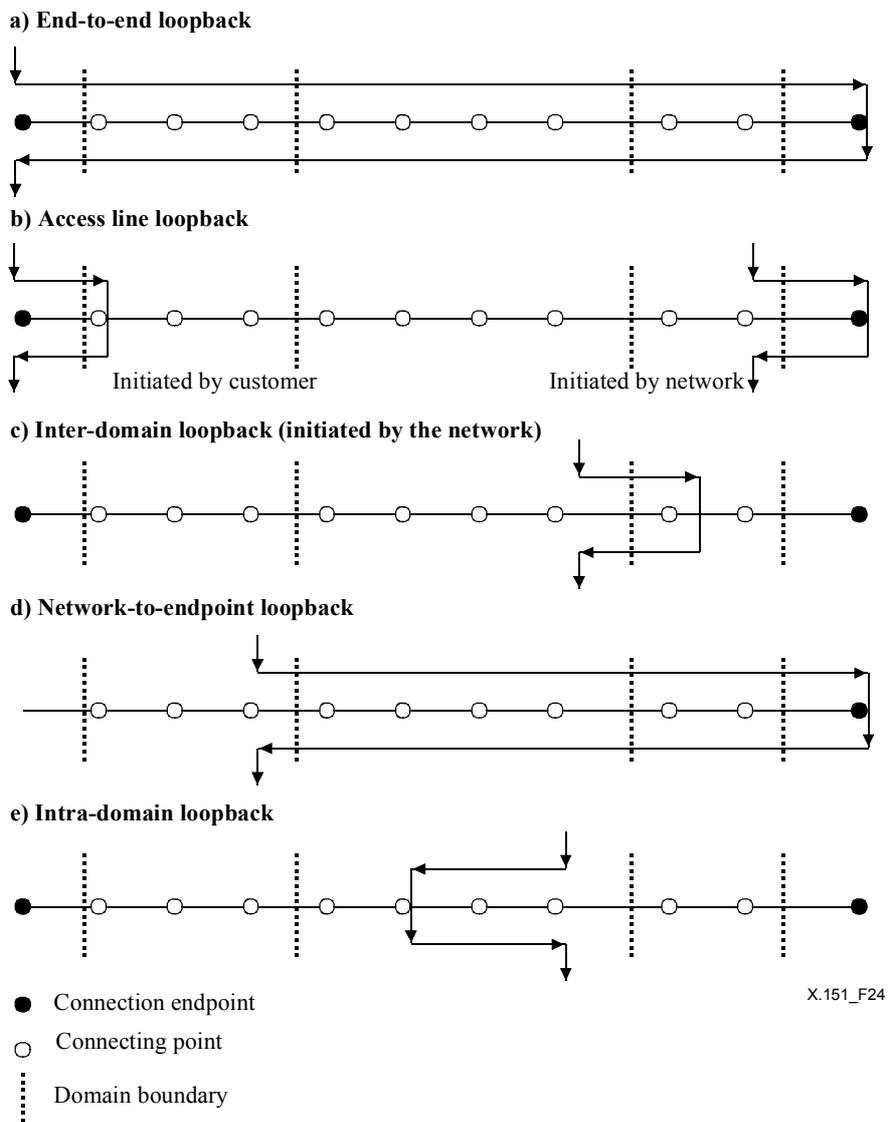
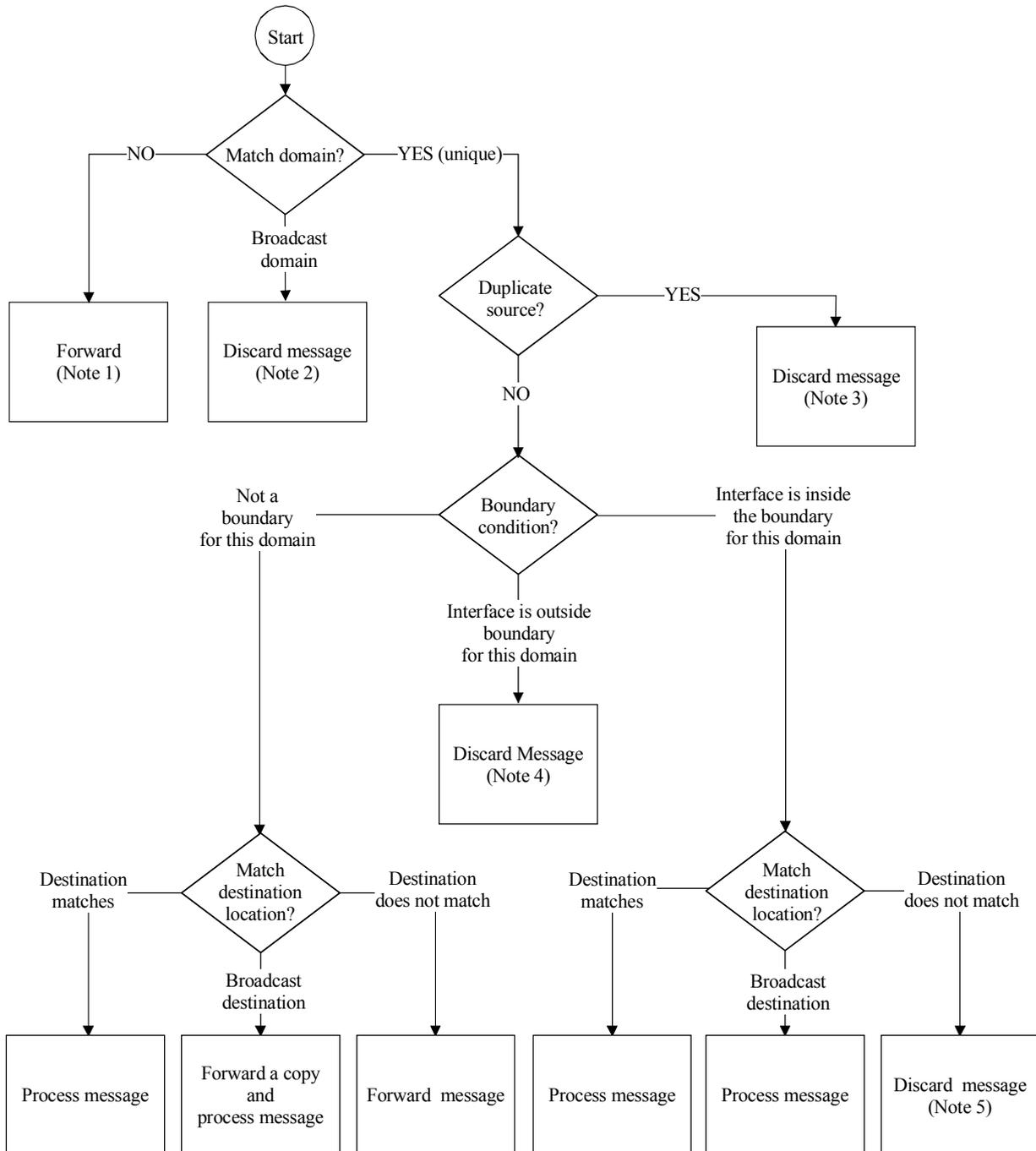


Figure 24/X.151 – Loopback applications

Appendix I

General receive procedures

The flow chart in Figure I.1 is illustrative of a possible implementation for OAM traffic arriving at an interface. If there is a conflict between this flow chart and the main text, implementations **should** follow the text.



- NOTE 1 – OAM devices must forward OAM messages addressed to foreign domains.
 NOTE 2 – Protocol error. It should be blocked.
 NOTE 3 – Duplicate identifier within domain. Logging to higher layer management may be desired.
 NOTE 4 – Security intrusion error. Logging to higher layer management may be desired.
 NOTE 5 – May be due to removal of FROMP from the circuit.

X.151_FI-1

Figure I.1/X.151 – General receive procedures

Appendix II

Message flows

This appendix contains informational examples of message flows between two peer OAM devices on a VC. If there is a conflict with the text of the main body of the Recommendation, the body of the Recommendation will supersede these examples.

II.1 Discovery

The Hello message is sent periodically; it contains the capabilities IF. Figure II.1 shows this sequence. Note that a subsequent message is allowed to add capabilities, but advertised capabilities are never withdrawn.

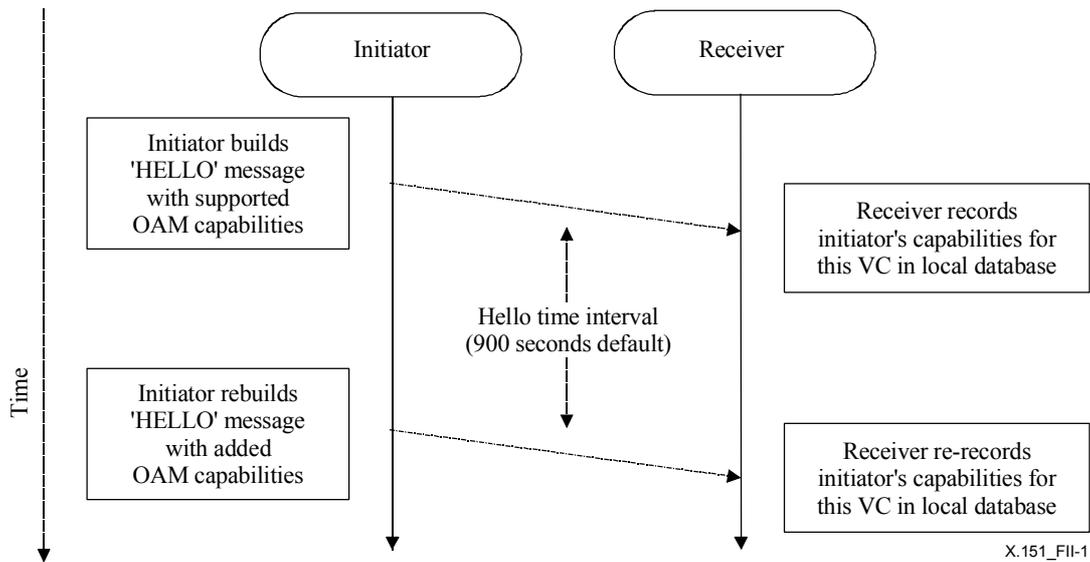
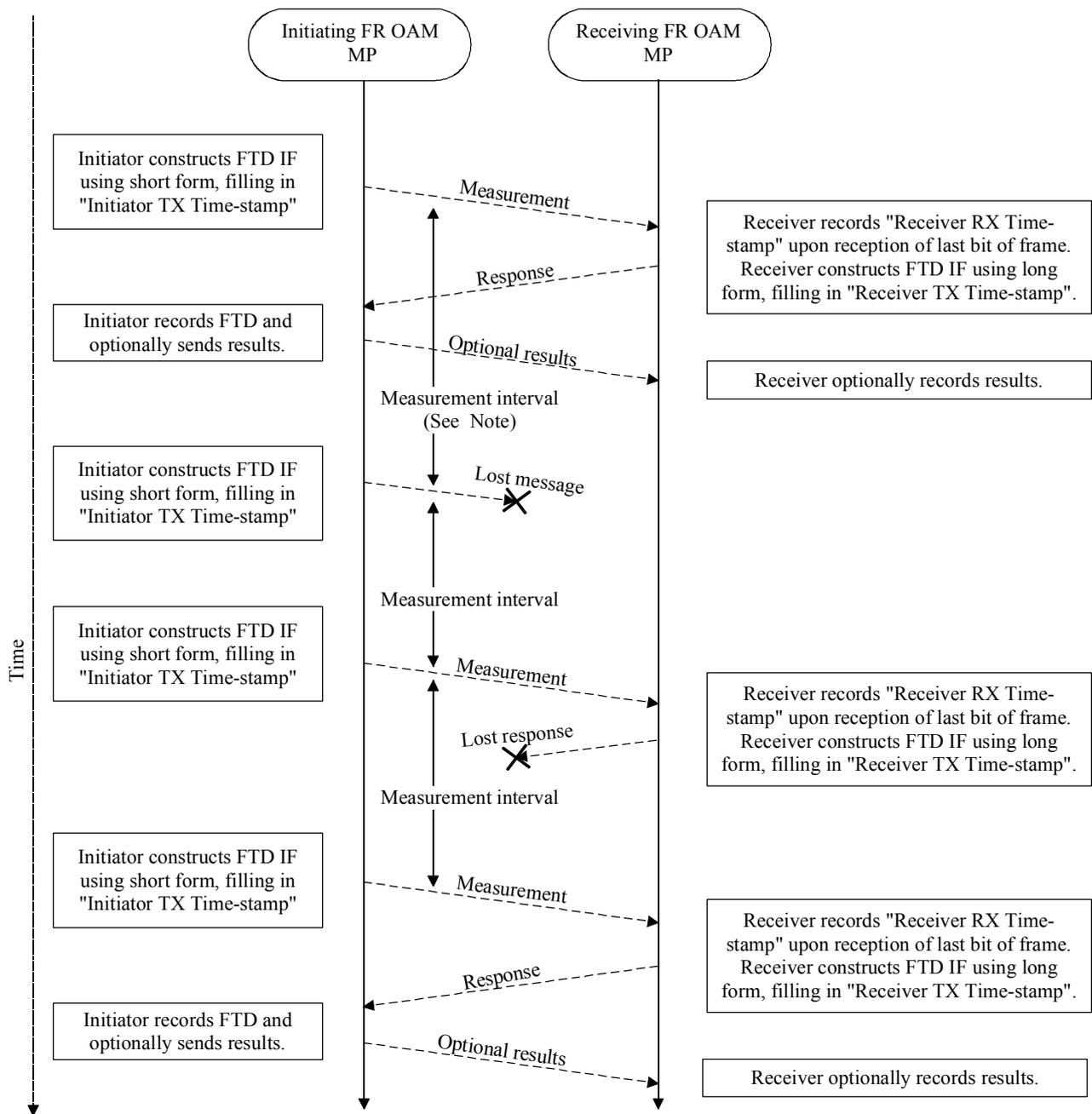


Figure II.1/X.151 – Hello message for discovery

II.2 FTD measurement

The FTD measurement can be done periodically. It requires a response as shown in Figure II.2.



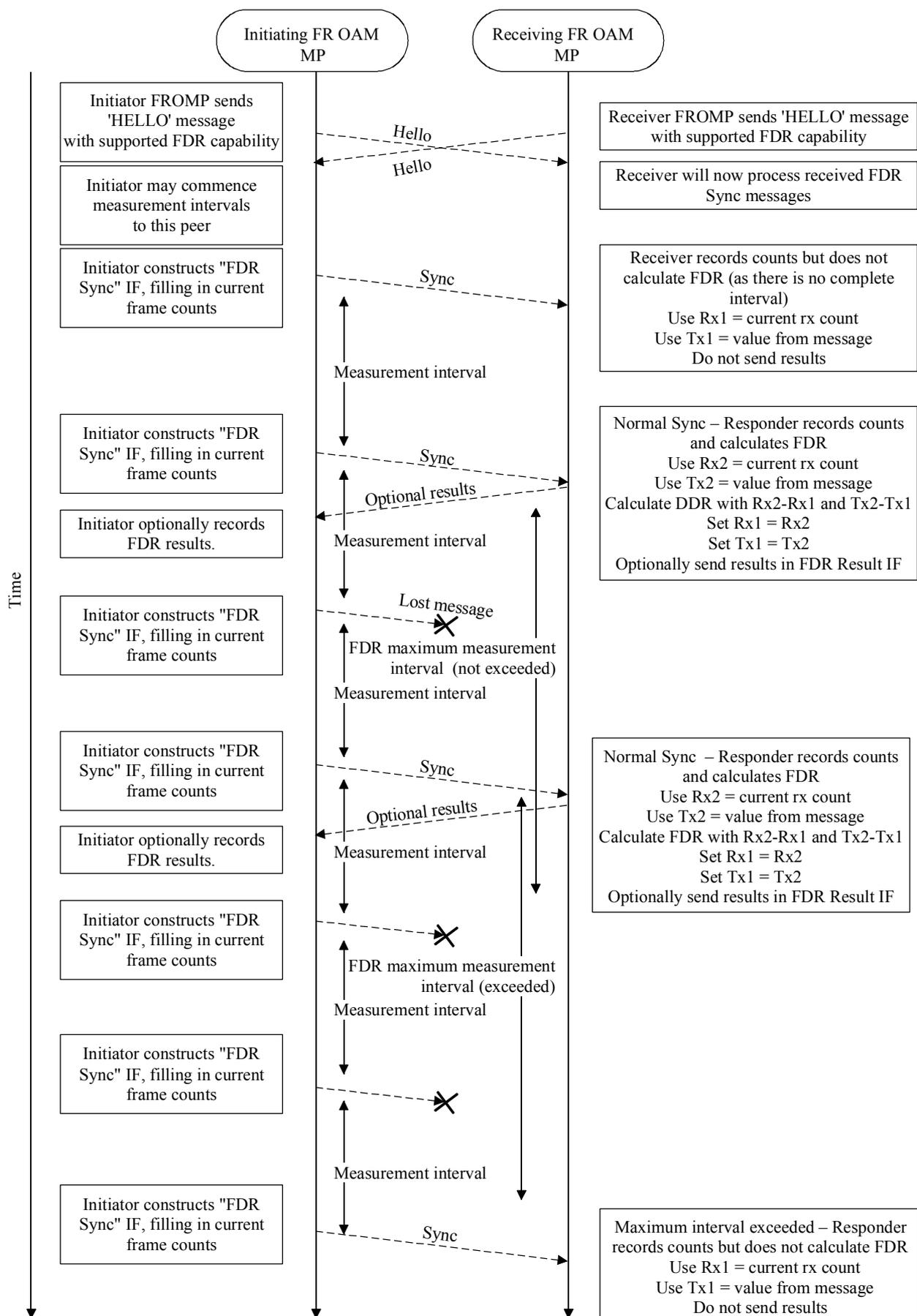
X.151_FII-2

NOTE – Measurement interval is set by TIMER-SLV-FTD

Figure II.2/X.151 – Frame transfer delay measurement

II.3 FDR/DDR measurement

The FDR and DDR measurements may be performed periodically. An example of a FDR sequence is shown in Figure II.3. The DDR measurement is done in the same fashion.



X.151_FII-3

Figure II.3/X.151 – FDR and DDR measurements

II.4 Non-latching loopback

An example of the message sequencing for a device using the non-latching loopback message is shown in Figure II.4.

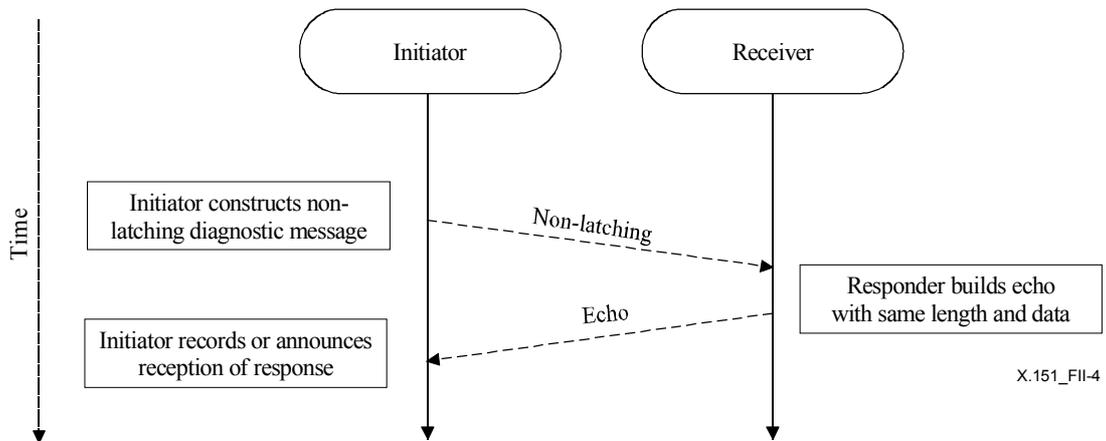


Figure II.4/X.151 – Using the non-latching loopback message

II.5 Latching loopback

Examples of message sequencing for a device using the latching loopback message are shown in Figure II.5.

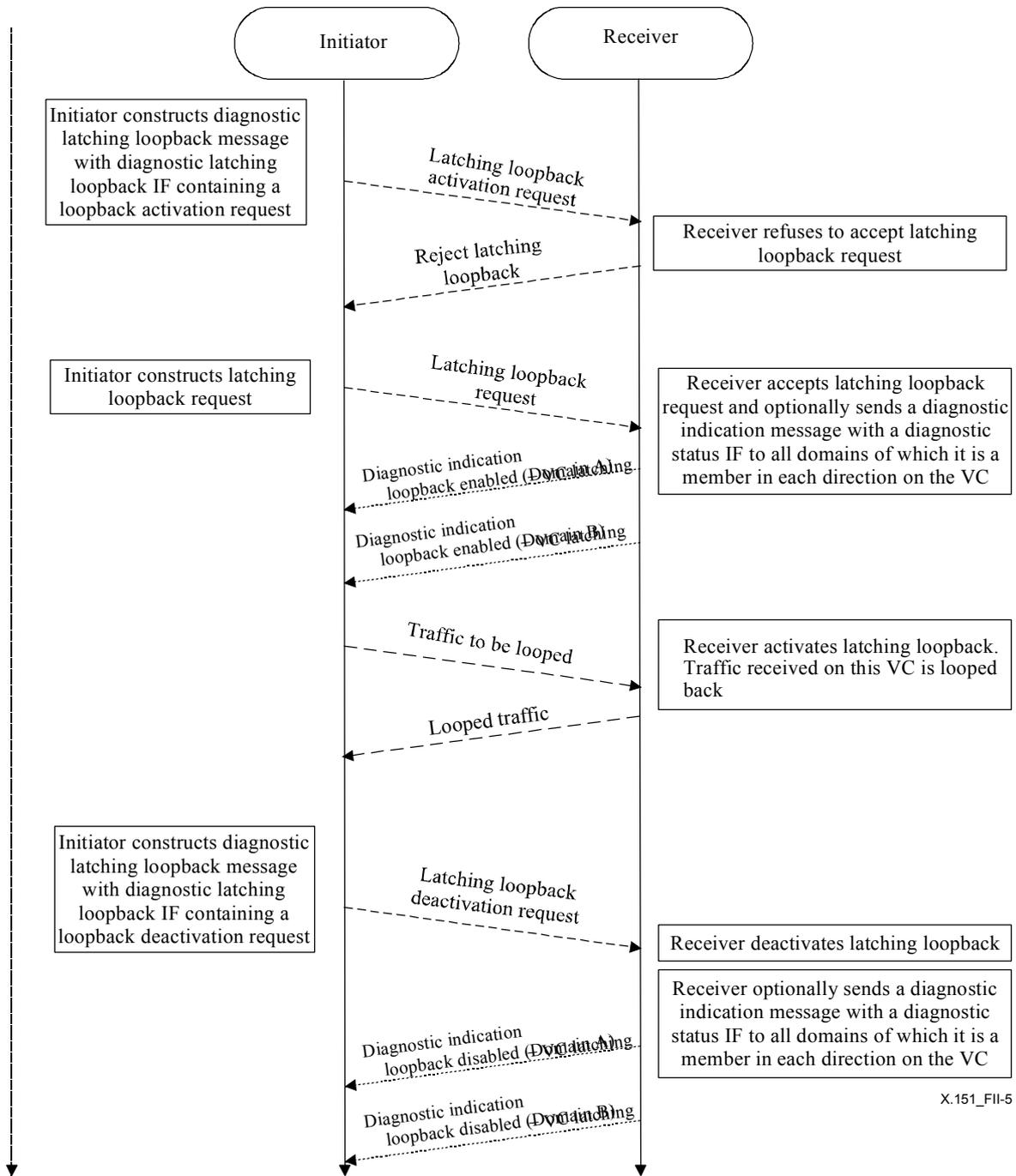


Figure II.5/X.151 – Using the latching loopback message

Appendix III

Example of delivery ratio calculation

The method used for obtaining frame delivery ratio and data delivery ratio results depends upon implementation-specific choices beyond the scope of this Recommendation. This appendix presents one method of obtaining the data to calculate these ratios. Other methods are possible.

Frame Relay Service Level Agreements (SLAs) include expectations for frame delivery ratio and data delivery ratio performance. Delivery success ratios are possible for several grades of traffic, as shown in Table III.1.

Table III.1/X.151 – Frame delivery ratio versus grade of traffic

Traffic grade	Description
Committed	frames transmitted to the network within the CIR
Excess	frames transmitted to the network in excess of CIR
Total	all frames transmitted to the network.

This appendix describes a procedure to calculate delivery success ratios for each of the grades using the messages defined by the frame relay OAM protocol. The procedure evaluates one-way delivery success between two Measurement Points (MP) in a network. The point where the frames enter the network segment is called the ingress MP. The point where the frames exit the network segment is called the egress MP. Refer to Figure III.1 for a reference diagram of a typical circuit where Location A₁ is the ingress MP and Location A₂ is the egress MP. The procedure is independently executed for the reverse one-way flow to produce delivery success ratios for both directions. In the example shown in Figure III.1, Location A₂ becomes the ingress MP for the reverse one-way flow.

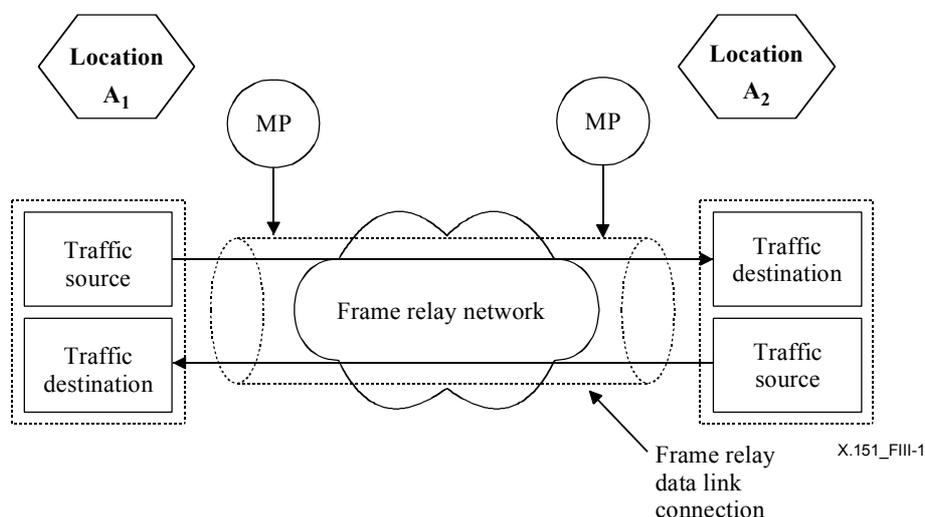


Figure III.1/X.151 – Reference connection for delivery ratio calculation

The operation of "delivery success" measurement occurs in time intervals determined by the ingress MP. The interval starts at T_0 following successful completion of the restart procedure (see 8.4.4.1 and 8.4.5.1) or at the conclusion of the previous interval. Interval duration (T_d) is

implementation-specific but bounded by counter-wrapping considerations. The egress MP uses received service verification messages containing a frame delivery ratio sync IF to detect the interval boundaries following completion of the restart procedure.

The following description of processing is focused on determination of frame delivery ratio results. The technique is applicable to data delivery ratio result calculation with the use of the appropriate service verification message information fields.

III.1 Ingress processing

The ingress MP determines the traffic grade of a frame. The method used to assign frames to particular traffic grades is implementation-specific. A discussion of traffic classification is provided in ITU-T Rec. I.370. This method does not rely upon an indication of the assigned traffic grade of each individual frame to the egress processor. The ingress MP maintains a frame count for each traffic grade. Upon detection of a frame within a given traffic grade, the frame count for that grade is incremented by one. At time T_d , a service verification message containing a frame delivery ratio sync information field is transmitted from the ingress MP to the egress MP.

The frame delivery ratio sync IF contains two fields: $FramesOffered_{Committed}$ and $FramesOffered_{Excess}$. The fields contain the frame counts for the corresponding grades. The counts will wrap back to zero periodically, the frequency determined by physical access speed, frame sizes, and frame arrival rates.

III.2 Egress processing

The egress MP counts frames exiting the network during an interval. A single count of total frames exiting the network is maintained, as the frames are NOT identified by traffic grade.

Upon receipt of a service verification message containing a frame delivery ratio sync IF, the egress MP performs the following actions:

The running count of total frames exiting the network during the interval is assigned to $\Delta FramesReceived$.

The $\Delta FramesOffered_{Committed}$ Count for the interval is computed by subtracting the value reported by the ingress MP at the end of the last interval from the value reported by the ingress MP in the just received service verification message. The calculation **must** detect and adjust for counter-wrap.

The $\Delta FramesOffered_{Excess}$ Count for the interval is computed by subtracting the value reported by the ingress MP at the end of the last interval from the value reported by the ingress MP in the just received service verification message. The calculation **must** detect and adjust for counter-wrap.

The total lost frame count for the interval just ended is calculated as follows:

$$\Delta FramesLost = (\Delta FramesOffered_{Committed} + \Delta FramesOffered_{Excess}) - \Delta FramesReceived$$

The counts of committed and excess frames delivered successfully are calculated as follows:

If $\Delta FramesLost \geq \Delta FramesOffered_{Excess}$

$$\Delta FramesDelivered_{Excess} = 0$$

$$\Delta FramesDelivered_{Committed} = \Delta FramesReceived$$

If $\Delta FramesLost < \Delta FramesOffered_{Excess}$

$$\Delta FramesDelivered_{Excess} = \Delta FramesOffered_{Excess} - \Delta FramesLost$$

$$\Delta FramesDelivered_{Committed} = \Delta FramesOffered_{Committed}$$

The Frame Delivery Ratio for the Committed Traffic Grade is calculated as follows:

$$FDR_{committed} = \Delta FramesDelivered_{Committed} / \Delta FramesOffered_{Committed}$$

The Frame Delivery Ratio for the Excess Traffic Grade is calculated as follows:

$$FDR_{excess} = \Delta FramesDelivered_{Excess} / \Delta FramesOffered_{Excess}$$

The Frame Delivery Ratio for the Total Traffic Grade is calculated as follows:

$$FDR_{total} = \Delta FramesReceived / (\Delta FramesOffered_{Committed} + \Delta FramesOffered_{Excess})$$

The counts of committed and excess frames lost are calculated as follows:

$$\Delta FramesLost_{Committed} = \Delta FramesOffered_{Committed} - \Delta FramesDelivered_{Committed}$$

$$\Delta FramesLost_{Excess} = \Delta FramesOffered_{Excess} - \Delta FramesDelivered_{Excess}$$

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems